

Windows® IT Pro

MAY 2010 | WINDOWSITPRO.COM | WEEKLY



Exchange 2003 to Exchange 2010

Step-by-Step

Exchange Migration

p. 26

High Availability:

Deploy Database
Availability Groups
in Exchange 2010 p. 38

Create Windows 7 Media
for Deployment p. 42

Build Active Directory
MMC Consoles p. 47

From 32-Bit to 64-Bit:
Understanding Processor
Architectures p. 51

**InfoPath 2010
with SharePoint 2010:**
Design a Data-
Collection Form p. 54

Exchange 2010
Virtualization p. 58

Transitioning to Exchange 2010:

Interview with Microsoft's
Rajesh Jha p. 35



**40% of employee
Internet access is
non-work related.**



How do YOU monitor, control and police it?

GFI WebMonitor™

Web Security, Web Monitoring & Internet Access Control

Increase network security and employee productivity by giving administrators control over what users are browsing and downloading in real time.

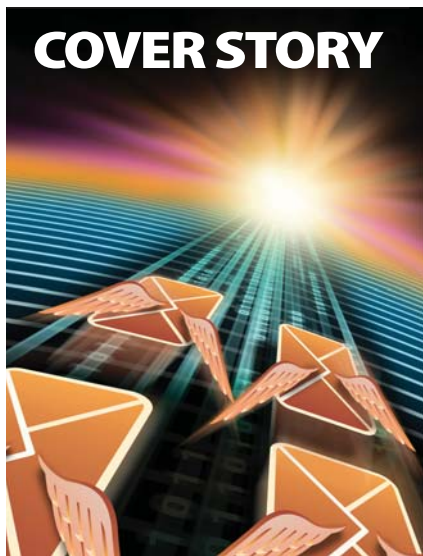
Stop: Spyware, Malware & Viruses!
Stop: Connections in real time!

Find out more, download your FREE 30-day trial and get a FREE baton*:

www.gfi.com/wwb



COVER STORY



26 Migrating from Exchange Server 2003 to Exchange Server 2010 – A Small Organization Perspective

Use these steps, easily scalable to larger deployments, as a guide so that you're fully prepared for the upgrade to Exchange 2010.

BY MICHAEL B. SMITH

Exchange on a Domain Controller 30

35 Microsoft Helps Smooth Your Exchange 2010 Transition

Microsoft's Rajesh Jha talks about transitioning to the company's latest mail server, whether on-premises or to Exchange Online, and gives advice about what IT shops should be doing now to plan for the move.

BY B.K. WINSTEAD

38 Deploying Database Availability Groups in Exchange Server 2010

After heeding some prerequisites, you're ready to create a DAG, add servers to it, and allow seeding and replication to complete. Here's how to tackle those steps.

BY PAUL ROBICHAUX

INTERACT

19 Reader to Reader

How to manage networks with Spiceworks, render web pages in a different language, manually uninstall an Exchange server, and use one PowerShell cmdlet to test for the existence of variables, files, registry keys, and more.

22 Ask the Experts

Learn to create Outlook Quick Parts, create SAN certificates, turn jumbo frames on in Hyper-V, audit file system actions, and more.

FEATURES

SOLUTIONS PLUS

42 Create Windows 7 Media for Deployment

With these step-by-step instructions, you can easily customize your Windows 7 installation media. You can change preferences such as installation languages, and even fully automate installation.

BY RHONDA LAYFIELD

47 Create Active Directory MMC Consoles for Down-Level Administrators

After you implement a least-privilege delegation model in Active Directory, you should use MMC to provide administrative tools to help administrators perform their delegated tasks.

BY DAN HOLME

51 What You Need to Know in a Mixed 32-bit and 64-bit Environment

When you transition from a 32-bit Windows environment to a mixed environment of 32-bit and 64-bit Windows, you need to understand processor architectures. You also need to look out for some potential pitfalls.

BY ALEX K. ANGELOPOULOS

54 InfoPath 2010 with SharePoint 2010: A Walkthrough

Get a sense of the power of InfoPath and SharePoint by building a custom form.

BY RYAN THOMAS

REQUIRED READING: VIRTUALIZATION

58 Going Virtual with Exchange 2010

Use these guidelines to deploy a fault-tolerant and high-performance virtual Microsoft Exchange Server 2010 environment with properly designed virtual hosts and guests and correct sizing for each of the server roles.

BY MICHAEL NOEL

IN EVERY ISSUE

7 IT Community Forum

79 Directory of Services

79 Advertising Index

79 Vendor Directory

80 Ctrl+Alt+Del

Windows IT Pro

A PENTON PUBLICATION

MAY_2010
VOLUME_16
NO_5

COLUMNS

CROCKETT | IT PRO PERSPECTIVE



6 Exchange Upgrade Creates Domino Effect

An IT pro who is upgrading to Exchange Server 2010 shares the driving forces behind the move and discuss the ways in which the transition affects other parts of the IT organization.

THURROTT | NEED TO KNOW



9 What You Need to Know About Windows 7, IE 9, Hotmail, Live Messenger, and More

Stay up to date on what's happening with Windows 7, Windows Phone 7, Office 2010, and NAC for the Internet.

MINASI | WINDOWS POWER TOOLS



11 Diskpart Goes Virtual

Learn how to use Diskpart to create and manipulate virtual hard disks.

OTEY | TOP 10



15 Windows Sysinternals Tools

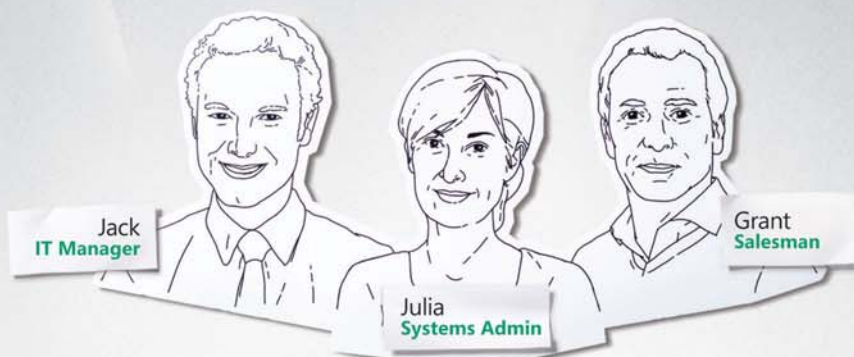
These favorite utilities will ease your Windows management by simplifying tasks such as keeping track of file shares, managing user log ons, and performing physical-to-virtual disk conversions.

GERBER | WHAT WOULD MICROSOFT SUPPORT DO?



17 Chasing the DNS Zone-Location Problem

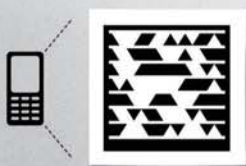
Learn how to recognize DNS zone-replication conflicts on your Active Directory-integrated DNS servers and solve the problem or avoid it altogether.



 *Drive efficiency and fuel inspiration where it strikes.*

Windows® 7 Enterprise Edition, Windows Server® 2008 R2, Microsoft® System Center and Forefront™ can help drive the success of your business. How, exactly? Well, when deployed together, they help streamline management of your desktops, minimize threats and data loss, while maximizing secure remote access and user productivity across applications, locations and devices. End result? Inspired users. Efficient business. Happy IT.

To learn more about the benefits of these products, go to itseverybodysbusiness.com/deploy



Snap this tag to get the latest news on deploying optimized desktops or text DEPLOY to 21710*

Get the free app for your phone at <http://gettag.mobi>

Because it's everybody's  business

PRODUCTS

65 New & Improved

Check out the latest products to hit the marketplace.

PRODUCT SPOTLIGHT: SpectorSoft **Spector Server 2010**

REVIEW

66 Paul's Picks

If you want Office 2010, you should get Office 2007 now; and how to get BitLocker-like data encryption at a low cost.

BY PAUL THURROTT

REVIEW

67 SolarWinds ipMonitor

SolarWinds' ipMonitor provides excellent general-purpose network monitoring, but the next version needs to overcome some flaws.

BY BRANDON CARSE

REVIEW

68 StarWind Enterprise HA Unlimited 5.0

StarWind turns the storage market on its ear by providing almost all the benefits of high-end SAN storage at a price that smaller businesses can afford.

BY MICHAEL OTEY

MARKET WATCH

69 The Rise of Cloud Computing

Cloud computing is a compelling, cost-cutting notion for many businesses. Here's what the major vendors are offering today.

BY MICHAEL OTEY

BUYER'S GUIDE

73 Group Policy Management Tools

Managing Group Policy requires all the help you can get. We've collected some useful solutions that will help you control, monitor, or extend Group Policy as you see fit.

BY CAROLINE MARWITZ

77 Industry Bytes

Explore an IT security wish list for the new decade and why the Droid is one editor's top choice for a device.



ON THE WEB

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at <http://tinyurl.com/d5bquf>. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Windows IT Pro

EDITORIAL

Editorial and Custom Strategy Director

Michele Crockett mcrockett@windowsitpro.com

Executive Editor, IT Group

Amy Eisenberg amy@windowsitpro.com

Technical Director

Michael Otey motey@windowsitpro.com

Senior Technical Analyst

Paul Thurrott news@windowsitpro.com

Custom Group Editorial Director

Dave Bernard dbernard@windowsitpro.com

Web and Developer Strategic Editor

Anne Grubb agrubb@windowsitpro.com

Systems Management

Karen Bemowski kbemowski@windowsitpro.com

Caroline Marwitz cmarwitz@windowsitpro.com

Zac Wiggy zwiggy@windowsitpro.com

Messaging, Mobility, SharePoint, and Office

Brian Keith Winstead bwinstead@windowsitpro.com

Networking and Hardware

Jason Bovberg jbovberg@windowsitpro.com

Security

Lavon Peters lpeters@windowsitpro.com

SQL Server

Megan Bearly Keller mkeller@windowsitpro.com

Sheila Molnar smolnar@windowsitpro.com

Production Editor

Brian Reinholz breinholz@windowsitpro.com

IT Media Group Editors

Linda Harty, Chris Maxcer, Rita-Lyn Sanders

CONTRIBUTORS

SharePoint and Office Community Editor

Dan Holme danh@intelliem.com

Senior Contributing Editors

David Chernicoff david@windowsitpro.com

Mark Joseph Edwards mje@windowsitpro.com

Kathy Ivens kivens@windowsitpro.com

Mark Minasi mark@minasi.com

Paul Robichaux paul@robichaux.net

Mark Russinovich mark@sysinternals.com

Contributing Editors

Alex K. Angelopoulos aka@mvps.org

Sean Deuby sdeuby@windowsitpro.com

Michael Dragone mike@mikerochip.com

Jeff Felling jeff@blackstatic.com

Brett Hill brett@iisanswers.com

Darren Mar-Elia dmarelia@windowsitpro.com

Tony Redmond 12knocksinna@gmail.com

Ed Roth eroth@windowsitpro.com

Eric B. Rux ericbrux@whshelp.com

John Savill john@savilltech.com

William Sheldon bsheldon@interknowlogy.com

Randy Franklin Smith rsmith@montereytechgroup.com

Curt Spanburgh cspanburgh@scg.net

Orin Thomas orin@windowsitpro.com

Douglas Toombs help@toombs.us

Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Production Director

Linda Kirchgesler linda@windowsitpro.com

Senior Graphic Designer

Matt Wiebe matt.wiebe@penton.com

ADVERTISING SALES

Publisher

Peg Miller pmiller@windowsitpro.com

Director, International and Agency Services

Don Knox don.knox@penton.com

EMEA Managing Director

Irene Clapham irene.clapham@penton.com

Director of IT Strategy and Partner Alliances

Birdie J. Ghiglione birdie.ghiglione@penton.com
619-442-4064

Online Sales and Marketing

Manager

Dina Baird Dina.Baird@penton.com

Key Account Directors

Jeff Carnes jeff.carnes@penton.com
678-455-6146

Chrissy Ferraro christina.ferraro@penton.com
970-203-2883

Account Executives

Barbara Ritter barbara.ritter@penton.com
858-759-3377

Cass Schulz cassandra.schulz@penton.com
858-357-7649

Client Project Managers

Michelle Andrews michelle.andrews@penton.com
970-613-4964

Kim Eck kim.eck@penton.com
970-203-2953

Ad Production Supervisor

Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

IT Group Audience Development Director

Marie Evans marie.evans@penton.com

Marketing Director

Sandy Lang sandy.lang@penton.com

CORPORATE



Chief Executive Officer

Sharon Rowlands Sharon.Rowlands@penton.com

Chief Financial Officer/Executive Vice President

Jean Clifton jean.clifton@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group

Kim Paulsen kpaulsen@windowsitpro.com

Windows®, Windows Vista®, and Windows Server® are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries and are used by Penton Media under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation.

WRITING FOR WINDOWS IT PRO

Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

PROGRAM CODE

Unless otherwise noted, all programming code in this issue is © 2009, Penton Media, Inc., all rights reserved. These programs may not be reproduced or distributed in any form without permission in writing from the publisher. It is the reader's responsibility to ensure procedures and techniques used from this publication are accurate and appropriate for the user's installation. No warranty is implied or expressed.

LIST RENTALS

Contact MeritDirect, 333 Westchester Avenue, White Plains, NY or www.meritdirect.com/penton.

REPRINTS

Diane Madzelonka, Diane.madzelonka@penton.com,
216-931-9268, 888-858-8851

3 TOP TECH INITIATIVES TARGETED BY FRAGMENTATION

As CIOs and IT managers gear up to meet the challenges of stringent budgets and new tech initiatives, how they handle file fragmentation will contribute to the difference between cost-effective consolidation and increased overhead.

Virtualization

Efficiency vs. "fragmentation on top of fragmentation"

The hard disk is the slowest component of a system's throughput. File fragmentation only makes the bottleneck worse. In the case of virtualization, the disk must do far more; it must support numerous simultaneous operating systems and a greatly compounded rate of fragmentation both on the logical disk and the virtual disks.

These virtual disk files fragment just as any other file can, resulting in what amounts to a "logically" fragmented virtual hard disk, which still has typical file fragmentation contained within it. In other words, virtualization brings about a "fragmentation on top of fragmentation" that can quickly cripple system speed and negate the efficiency virtualization is designed to deliver.

Data Storage Management on SAN Devices

Is fragmentation still really an issue?

A storage area network (SAN) provides the ability to make remote disks appear to be local. SAN storage virtualization involves the creation of a usually very large, logical pool of data. Via software, that pool appears to be physically located all on one server. In actuality, that data may be located across hundreds of physical disks spread across dozens of servers.

The local disk file system does not know of and cannot control the physical distribution or location in a virtualized storage environment. As a result of fragmentation, NTFS has to make multiple requests regardless of the physical or virtualized storage environment.

SANs cannot address file system level fragmentation and neither can proprietary architectures or data retrieval technologies. The overhead on the operating system is heavily impacted by fragmentation. *Local disk file defragmentation is vital.*

The Standard Operating Environment

Lowering network operating costs with efficiencies of scale

There are multiple dynamics that make up overall network efficiency but because file fragmentation is created at the operating system level regardless of how much free space is on the disk, its negative effect on the network is one of the most basic issues to resolve. When not effectively addressed, fragmentation creates a perfect storm of network issues including:

- Slow read/write times
- Slow backups and higher failure rates
- Database lockups

- Shorter productive disk life
- Spiraling energy costs
- Slow boot time
- Increased Help Desk traffic
- Higher re-imaging costs

Resolving fragmentation at base image level would clearly make sweeping improvements to a network, lowering the cost of ownership with the least amount of effort.

The Economics of Fragmentation Prevention

Diskeeper® 2010 technology and the system performance paradigm

Eliminating fragmentation as a performance issue has four basic goals: the reestablishing of optimum performance, reliability, longevity and energy efficiency in every system on a network. Only Diskeeper 2010 includes the innovative functionality to achieve this:

- It prevents up to 85% of all fragmentation before it occurs
- It eliminates any remaining fragmentation in real time
- It quickly handles even the largest mission-critical enterprise servers
- It is completely automatic and invisible
- It includes a centralized graphical administration console scalable to any size

In reality, since every system fragments, any global solution must meet stringent requirements or its operational overhead will negate gains. Diskeeper 2010, with an edition for every Windows® system from laptops to the largest mission critical enterprise servers, is the only solution that increases performance and lowers total cost of ownership at the same time.

Diskeeper

The only way to prevent fragmentation
before it happens™



Special Offer

Try Diskeeper 2010 FREE for 45 days!

Download at www.diskeeper.com/specialtrial

(Note: Special 45-day trialware is only available at the above link)

[Volume licensing and Government / Education discounts are available from your favorite reseller or call 800 829-6468](#)



"IT pros contemplating an upgrade should examine the changes in architecture between Exchange 2007 and Exchange 2010."

Exchange Upgrade Creates Domino Effect

Upgrading to Exchange 2010 affects more than just email

Last fall at our Windows Connections conference in Las Vegas, *Windows IT Pro* held a small workshop for IT pros whose organizations were just beginning to plan their migration to Exchange Server 2010. I recently checked back in with a few attendees to see how their upgrades were going. One IT pro said his company had abandoned any immediate plans to migrate, but two others were in the thick of the transition. Pam Dudley, a systems administrator for a Nashville-based law firm, shared her insights about her organization's reasons for the upgrade and lessons learned in the planning process.

Dudley said that the high-availability features of Exchange 2010 were hands-down the biggest driver for her company's upgrade. "Our Exchange data has grown at such a rate that we're really just running out of room," Dudley said. "We've just gotten a new SAN up and running, and with the conversion to Exchange 2010 we've been charged with moving storage from local machines to the SAN. We're also looking at virtualizing Exchange. So this one product migration has become a huge project encompassing other things."

One of the factors affecting the Exchange migration is a new document-management system the firm implemented; this application allows workers to transfer client documents directly from Exchange. Very few documents at the law firm now exist in physical form.

In addition, IT organizations need to plan and deploy new data-retention policies as a result of new regulations such as the Health Information Technology for Economic and Clinical Health Act (HITECH), which expands the reach of the Health Insurance Portability and Accountability Act (HIPAA) to include business associates of the entities that are subject to HIPAA. "We have to keep this data secure, and we have a number of protocols to follow that we didn't before," Dudley said.

The Exchange upgrade has caused Dudley's organization to reassess other initiatives and launch related projects. The company is trying to reduce hardware by removing mailboxes from physical servers and putting them on the SAN. The company's virtualization strategy is still in the planning stage. "There is some debate at this point about exactly how much of the Exchange system we're going to virtualize," Dudley said. She's also reviewing which workloads to put on the virtual machines and which to put on the physical servers.

In addition to scrutinizing their virtualization strategy, Dudley said that the rollout of Outlook 2010 will be a significant factor

for the organization because of the ties to their new document-management system. "I know that with Exchange 2010, the functionality available to you is dependent on the Outlook client you use, and we're still on Outlook 2003," Dudley said. "The further back you go with the client—the further away you get from the current Exchange server—the more functionality you lose on that Exchange server. And of course with Outlook, we have to wait on the third-party vendors for the snap-ins so they can also work."

The other piece of the Exchange upgrade puzzle is preparing Active Directory (AD) for the migration. Although Dudley said she's familiar with the AD cleanup needed because of the organization's previous migration, the current project has caused her organization to reassess its Windows Server deployment as well. Most of the firm's servers are running Windows Server 2003, but Dudley is targeting certain machines for upgrades. "We currently have one AD server that's on Windows Server 2008 and we're going to move that to R2," Dudley said. "We're going to bring up an additional domain controller on Windows Server 2008 R2. We'll take the other Windows Server 2003 machines out of the mix so that we have the AD forest on Windows Server 2008."

The other rollout that will follow closely behind the Exchange 2010 migration is an upgrade to Windows 7. "But we've got to have 2008 to take advantage of some of the opportunities Windows 7 offers in efficiencies."

Aside from emphasizing that many other systems will be connected to an Exchange 2010 migration, Dudley advises IT pros contemplating an upgrade to closely examine the changes in architecture between Exchange 2007 and Exchange 2010. "It will change how you allocate roles, how you allocate resources, and how you do your planning," she said. "The parts of the new architecture that are different are very different."

Dudley is planning to complete the upgrade to Exchange Server 2010 by the third quarter of this year. Although the migration itself will be fairly straightforward, the year clearly will be packed with challenges as she navigates the changes that the Exchange migration will cause to other systems.



InstantDoc ID 104627

MICHELE CROCKETT (michele.crockett@penton.com) helped launch *SQL Server Magazine* in 1999, has held various business and editorial roles within Penton Media, and is currently editorial and custom strategy director of *Windows IT Pro*, *SQL Server Magazine*, and *System iNEWS*.

■ Script Editors
■ Exchange Storage

■ System Idle
■ PowerShell Tips

LETTERS@WINDOWSITPRO.COM

iTripoli Response

I want to thank Michael Otey for his review of iTripoli's Admin Script Editor ("Pair of PowerShell Editors Pack a Punch," March 2010, InstantDoc ID 103483). I'm compelled to point out a couple things. Unlike with development languages, we don't feel administrators should be concerned with "projects" and collections of files, so we've worked to remove the requirement. ASE lets you store all the script-specific settings you want in the script so that you aren't concerned with multiple files. For example, our ScriptForm Designer writes and reads code directly from the script and doesn't require a separate file that must be used to open saved forms for editing.

Often, when you see a long list of supported languages, the offered feature is simple keyword highlighting. We provide much more than this by focusing on the languages that matter to administrators. For example, our many code wizards support PowerShell, VBS, KiXtart, and Autolt.

ASE 3.5 supports everything on Windows 7 except the PowerShell debugger. We have hundreds of users running ASE on Windows 7 today. But our official support for Windows 7 and 64-bit systems will be out soon, including native 64-bit script packaging.

We have indeed received feedback that our "special" icons aren't always appreciated. Therefore, we include a second set of icons that can be easily selected in ASE Options. To make sure everyone can make ASE look the way they like, we've provided several customization options for adjusting colors, layout, and icons, and users can even group or eliminate windows. We've posted a YouTube video (www.youtube.com/watch?v=LBDMDnZaKd0) that runs through these settings.

It's unfortunate that Michael had concerns with ASE reformatting his code. This is another feature we've invested heavily in that's typically considered an asset: The

ScriptFormatter automatically inserts tabs and spaces according to fully customizable rules. Any of these rules can be edited or disabled, and the entire feature can be turned off.

If a window is inadvertently closed, it can be quickly restored by selecting Restore Default Layout from the formatting section of ASE Options or by choosing the specific tool you're looking for from the Window menu at the top of the screen.

Remember that quick comparisons tell only a fragment of the story. To truly understand differences between products, you need to get your hands on those products. For example, our Logon Script Builder is an extensible drag-and-drop environment whereas other solutions might offer no more than a simple wizard that provides limited functionality.

—Bob Kelly
iTripoli

Thanks for your comments! You have a great product. I liked all the things it does to make scripting easier and more approachable for the administrator. Regarding multiple file projects, I meant projects that are composed of multiple related script files grouped together under a project name. You open the project, and that opens all the related files so that you work on them as a group. I wasn't referring to your ScriptForm Designer. I liked the way that worked.

Regarding languages, your point is well taken. The product has full support for the languages you list. However, for marketing purposes, I would suggest listing the broader set, even if most users will use only a subset of them.

About the formatting, I've inherited scripts from all over and they're formatted every which way. I don't want to even attempt to apply a standard to them. I just want to edit them as they are and go on to the next thing. ASE seems to always want to reformat the scripts rather than just follow the formatting that's present.

IPv6 Implementation

Mel Beckman's "IPv6 Hands-On Lab Setup Guide" (March 2010, InstantDoc ID 103361) is great. I hope everyone takes advantage of it—if only to increase the traction that IPv6 so desperately needs in the real world. IPv6 needs all the awareness it can get.

—Michael Dragone

ASE is a good product. I especially appreciate the information about the icons. I wasn't aware I could change them. When you offer Windows 7 debugging support, I'm there. I'm sure we'll revisit this topic in the future.

—Michael Otey

Exchange Storage

I enjoyed Lee Dumas's article, "Exchange Storage: DAS vs. SAN vs. iSCSI" (January 2010, InstantDoc ID 103013). In the section about RAID levels, he mentions, "The performance of RAID 5 is about a third of that of RAID 1 and 0+1, because each write to the OS requires three writes to disk." I agree with that statement with regard to writes, but it should be emphasized that RAID 5 has another important performance benefit.

I've worked with ISAM, Pervasive (formerly Bettrieve), and Microsoft SQL Server accounting software databases for many years in the SMB market space. Generally, data table lookups, reporting, and backups (i.e., reads) are the most common disk-intensive activities in these applications. Common knowledge—that is, Wikipedia—says that RAID 5's read performance (i.e., striping with parity) is almost as good as that of RAID 0 for the same number of disks. Except for the parity blocks, data distribution over the disks follows the same pattern as RAID 0 (i.e., simple striping). RAID 5 is slightly slower with writes only because the disks must skip over the parity blocks.

Given the major benefit of data-loss protection that RAID 5 provides over RAID 0, RAID 5 is highly recommended in certain environments for database files (not including transaction logs).

—Bret A. Bennett

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Monitoring Uptime

Frank Bernard's letter (IT Community Forum, April 2010) in response to my FAQ "What's a fast way to find how long my system has been running?" (February 5, 2010, InstantDoc ID 103540) suggested using Task Manager's System Idle Process counter as a solution.

I was curious about this suggestion, so I did some testing. I found that the System Idle time is essentially the amount of time the CPU has been idle. On a busy box, this counter wouldn't be accurate. However, the results are even worse than that in a multicore machine because the counter considers each core's time. So if I had four idle cores, the System Idle time would increase four seconds for each second. (Make sure you enable the *Show processes from all users* option to see System Idle.)

The results from my 16-core server (well, eight hyperthreaded) showed a much longer System Idle time than it has actually experienced. Every second, the System Idle time increased by 16 seconds (idle server). The idle time showed the server as being up for 53 days (1272 hours). In reality, it had only been three days.

—John Savill

PowerShell Tips

It's nice to see more and more useful articles about PowerShell, such as Bill Stewart's "Running PowerShell Scripts Is as Easy as 1-2-3" (InstantDoc ID103427). I found out many of these things the hard way. I'm still a newbie, but I figured out one very useful method.

I've chosen to leave my security at the "restricted" level on my PC and all the PCs I support in my department. It's actually simple to reduce security to "unrestricted," run a script, and then set it back to "restricted." It requires running PowerShell from a regular Cmd wrapper, as you see in Listing 1.

The two variables for preferred workDrv and workDir need to be set. From there, all you have to do is run it. It prompts for the name of the script. I always copy the name beforehand. When prompted, I simply right-click to paste (Cmd QuickEdit feature), and hit Enter. The pause at the end lets me verify that the "restricted" policy has been reinstated properly. This can be tailored to run scripts on remote machines also.

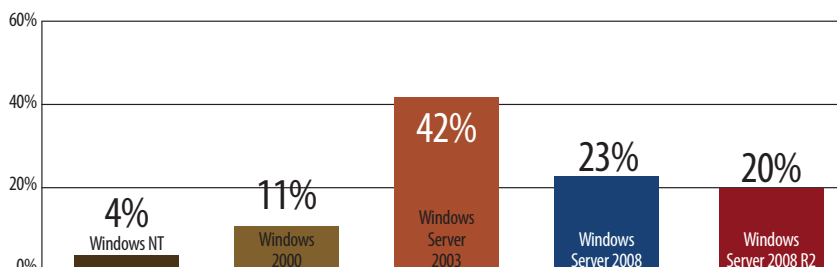
—Jeff O'Reilly

InstantDoc ID 104645

Listing 1:

```
Set workDrv=D:
Set workDir=Scripting\\Powershell
%workDrv%
Cd %workDrv%\%workDir%
Powershell -command "& {Set-ExecutionPolicy -Scope LocalMachine Unrestricted -Force}"
@Echo.
@Echo.
@Set /p ScriptName=What's the name of your PowerShell script? :
Powershell -command .\\%ScriptName%
@Echo.
@Echo.
:: Return the security policy to the defaults.
Powershell -command "& {Set-ExecutionPolicy -Scope LocalMachine Restricted -Force}"
Powershell -command "& {Set-ExecutionPolicy -Scope CurrentUser Undefined -Force}"
Powershell -command "& {Set-ExecutionPolicy -Scope Process Undefined -Force}"
:END
@Pause
```

Instant Poll Results: What versions of Windows Server are you running in your production environment?



Source: Windows IT Pro Instant Poll, www.windowsitpro.com, March 2010



How You Can Be More Green with Your Computing

Organizations can reduce their overall impact on the environment by judicious application of technologies such as power plans, migrating fax, implementing virtualization, and moving towards more efficient client hardware platforms. Listen to this podcast to learn more.

windowsitpro.com/go/GreenComputing

Tackling Security Challenges—May 12, 2010

With the explosion of Internet-connected services and the accompanying larger attack vulnerability, security has become an area of major focus for every organization. In this free conference, we'll drill down into the major security challenges organizations face today with their Microsoft-based services—and their organization in general—and examine solutions to common security frustrations. You'll also learn how virtualization affects your security picture. Register today for this free virtual conference this month.

windowsitpro.com/go/SecurityOnlineEvent

System Management Moves to the Cloud

The SMB market (500 to 3,000 desktops), can greatly benefit from a comprehensive systems management program. But finding a way to implement such a program without breaking the budget can be daunting. Simplify Your Systems Management! This free "how-to" essential guide is a must-have for SMBs.

windowsitpro.com/go/DesktopInTheCloud





"Starting over fresh with Windows Phone was the right thing to do. There wasn't any way that Windows Mobile was going to evolve into something competitive."

What You Need to Know About Windows 7, IE 9, Hotmail, Live Messenger, and More

This month marks a dramatic change in the format of this column. Instead of focusing on one or two major topics, I'll be taking a broader view of what's going on in the industry, with an eye towards those technologies that will impact individuals as well as organizations. I suspect we'll tweak things, so let me know what you think by emailing me at paul@thurrott.com. My goal, as always, is to provide you with timely information you can actually use.

Windows 7

With Windows 7 in the can and racking up some impressive sales numbers—Microsoft will have sold well over 100 million units by the time you read this and expects to ship over 300 million units in calendar year 2010—the Windows Division is turning its attention to various updates that will keep the momentum going this year.

First up is Windows 7 SP1. Microsoft still plans to deliver this update in Q4 2010, or roughly one year after the General Availability (GA) date of the initial Windows 7 release. My understanding is that SP1 will aggregate all of the software updates from that first year, and it might include driver support for new technologies (think USB3). But for Windows Server 2008 R2, SP1 is going to be a big, big deal from a functional perspective. More on that when I'm at liberty to reveal what's going on.

Internet Explorer 9

Equally important, perhaps, is Internet Explorer (IE) 9, though I don't expect to see the final version of this browser in 2010. Microsoft delivered a bare-looking IE 9 Platform Preview at its MIX'10 developer show in Las Vegas (and I think the public beta will ship by the end of the summer). But don't be fooled by the lack of interesting new UI in the IE 9 Platform Preview. IE 9 is essentially a brand new browser, the most radically remade version of the browser that the company has ever shipped. There are three key themes to this release: performance, real-world compatibility with actual web standards like HTML 5, CSS3, and SVG vector graphics, and hardware-accelerated graphics. Keep your eyes on this one.

Microsoft will also provide massive updates to its Windows Live Essentials application suite, which "lights up" or "completes" Windows 7, and to Hotmail, which is, by far, the most popular web-mail service on Earth. Both of these are important and will ship this year.

Hotmail and Windows Live Wave 4

Taking a public communications cue from Windows 7, the Windows Live team—which is indeed now part of the wider Windows division that's run by Steven Sinofsky—has been quiet for the past year. In fact, it's been too quiet. But that's by design, and we can expect a set of Windows Live Wave 4 releases this year that will encompass major updates to online services (like Hotmail) as well as the client-side applications that form Windows Live Essentials.

Why is this important? Microsoft has repeatedly stated that Windows Live "completes" Windows 7 and "lights up" underlying technologies and capabilities in its latest OS. That's a cute way of saying that Windows Live—especially Windows Live Essentials—"completes" Windows 7. That's because applications that used to be part of Windows—like Mail, Messenger, Movie Maker, Photo Gallery and others—have been stripped from the OS and are now only available as add-ons. This strategy is a mistake, I think. But that's the way it is.

Because of the cone of silence, all we have to go on right now are various leaks of Windows Live Essentials Wave 4. What we see is a ribbonization of the client-side applications—like Windows Live Mail and Photo Gallery—that previously sported traditional menus and toolbars. Windows Live Photo Gallery will support facial recognition via "face detection" and "face recognition" features, allowing you to tag faces and have the software auto-find other pictures of the same people. Photo Gallery will also sport a Photo Fuse feature that creates a single good photo from a set of pictures that all have flaws. (So you could, for example, remove people from a set of shots of a landscape.)

Microsoft's instant messaging (IM) application, Windows Live Messenger, is being expanded dramatically as a hub for the various Windows Live services, as well as third-party social networks. There's a browser add-on called Messenger Companion that

Microsoft's instant messaging application, Windows Live Messenger, is being expanded as a hub for Windows Live services.

provides IM and sharing capabilities from any website, and a full web client called, of course, Web Messenger.

There's even less information about the next Hotmail. Microsoft has begun previewing its plans with a small promotion on the Hotmail web site called "The New Busy." There's no real information per se, but it seems to point to the fact that the next Hotmail will focus on email overload and other productivity issues. Stay tuned.

Office 2010 Ship Date

Speaking of products that will ship in 2010, Microsoft plans to ship Office 2010 (and SharePoint 2010, Visio 2010, and Project 2010) to businesses worldwide on May 12. My sources tell me that the consumer launch (or GA) date is June 15. If you're waiting to buy Office 2010 for yourself, don't. Instead, buy Office 2007 now and take advantage of Microsoft's Tech Guarantee—if you purchase Office 2007, or a new PC with Office 2007, and activate it between March 5, 2010 and September 30, 2010, you can download the corresponding Office 2010 version for free. The only caveat: You must redeem this offer by October 31, 2010.

Essential Business Server Axed

Microsoft discontinued Essential Business Server (EBS). Let's ponder two interesting bits of information around that. First, customers who bought into this complicated mess of a product can get the individual component software (i.e., Windows 2008, Exchange Server 2007) from the EBS 2008 suite for free (minus local taxes, shipping and handling charges). This offer runs from June 30, 2010 through December 31, 2010, and if you're an EBS customer, you'd be crazy not to take advantage of it.

Second, Microsoft's sudden and unexpected EBS cancellation is, I think, an indication that its customers are turning to cloud-based solutions like Microsoft Online Services (MOS) and Business Productivity Online Suite (BPOS) even faster than expected. And this, I also think, will have huge implications for Windows Small Business Server (SBS). I thought it was a big mistake for Microsoft not to provide some sort of cloud-based SKU for SBS 2008 (where Exchange, at least, was a hosted service instead of on-premises). Mark my words: They won't make that mistake in the next version. The death of EBS proves this, as hosted solutions make even more sense for smaller environments. (Microsoft has issued a "no comment" on SBS 2008 R2, though the company tells me it is actively working on "the next version of SBS 2008.")

Microsoft's arch enemy, Google, already has the Google Apps product, which combines Gmail, Google Calendar, Google Docs, and other services into a free or very cheap online service that any small business can afford. And Google recently augmented this offering with the Google App Marketplace. Yeah, I know that "app store" is just this year's fun tech keyword (like "Linux" or "XML" from years past), but platforms matter. And when you're building a platform, the more apps the better. Google's marketplace is pretty slim as I write this. But Microsoft doesn't even have one for its own hosted services. Not yet anyway.

Network Access Control for the Internet

Microsoft raised a curiously controversial topic at the RSA Conference 2010, and I think it bears investigating. Why, asked Microsoft Corporate Vice President Scott Charney, can't we implement technology like Network Access Control (NAC) for the public Internet? It makes sense: NAC prevents PCs that don't meet an organization's security policies from joining the corporate network; instead, they are shunted off to a separate network where they are updated until compliant. If we could implement this on the Internet, it would prevent people with no common sense from infecting others with viruses and malware. The catch is that such a scheme is complicated and expensive. I think it's a great idea: Security should be job-one online.

Windows Phone 7 VS Apple

Windows Phone 7 is set for a September 2010 launch—and I think Microsoft has a winner on its hands. Starting over fresh with Windows Phone was the right thing to do. There wasn't any way that Windows Mobile was going to evolve into something competitive. Give Microsoft credit for simply killing off Windows Mobile 7.0. The company bet the bank on a relatively unknown UI. That UI, code-named Metro in its Windows Phone 7 incarnation, started in 2001 as Freestyle, the UI that became the first version of Windows Media Center. It's been improved over the years, and subsequent versions appeared in Portable Media Center (also forgotten), various generations of Windows Media Center, and, most recently, in the Zune PC software and Zune HD portable media player. So while few people have actually used Metro's predecessors, it's mature and ready to take on the mobile-using public. I think it has a chance to make a dent in other markets, including the living room (Xbox, Zune, Media Center, Mediaroom) and even the desktop PC.

Metro is more innovative than anything Apple is doing this year. Sure, Apple fooled customers into thinking that its iPad tablet is "magical and revolutionary" when it's really just a large iPod touch. But providing another way to access the same applications and online content as all its other devices isn't revolutionary. In fact, Apple's milking the iTunes ecosystem in a rather shameless way. It's the type of thing Microsoft has done, and what one might expect from a company that's too busy protecting its lead to do something that makes sense for customers. This is an opening, not just for Windows Phone but for other smartphone and device platforms that seek to challenge the Apple hegemony. Someone needs to do it.



InstantDoc ID 103689

PAUL THURROTT (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).



"Diskpart lets you use Windows Explorer to work with VHDs as if they're physical hard disks."

Diskpart Goes Virtual

The tool is great for not only your physical disks but also your imaginary disks

Over the past two months—in “Initializing Windows Disks with Diskpart” (InstantDoc ID 103422) and “Formatting and Resizing Partitions with Diskpart” (InstantDoc ID 103539)—I’ve showed you how to use Diskpart to wipe a hard disk clean, partition it into volumes, give those volumes drive letters, and format those drives. That’s all useful stuff to know, but IT pros increasingly find themselves concerned not only with real hard disks but also with *virtual* hard disks. Microsoft’s virtualization tools (e.g., Hyper-V, Windows 7’s XP Mode) need some standard way to package the “imaginary” hard drives that their virtual machines (VMs) rely on, and that standard is the Virtual Hard Disk (VHD) file format.

Pick apart a VM built with one of Microsoft’s VM-management offerings (e.g., System Center Virtual Machine Manager—SCVMM), and there’s at least one VHD hiding in there. And it’s not only VMs that use VHDs: Microsoft’s Complete PC Backup tool stores its backup files as VHDs. Further, VHDs are a great way to package a bunch of files and folders into just one file; it’s sort of like a .zip file, but unlike .zip files, VHDs can store NTFS attributes and security permissions. In fact, one of Windows 7’s and Windows Server 2008 R2’s more interesting new features is the ability to boot from VHD files whose virtual hard disks contain bootable OSs!

So, VHDs are here to stay, and I don’t know about you, but whenever a new file format becomes prevalent, I start looking around for diagnostic and configuration tools that understand that file format. In Windows 7 Enterprise, Windows 7 Ultimate, and Server 2008 R2, that tool is Diskpart. With Diskpart, you can create VHDs from scratch or examine existing ones and give them drive letters so that you can use Windows Explorer to work with them as if they’re physical hard disks.

Let’s start examining Diskpart and VHDs by seeing how to create a VHD. From inside Diskpart, the command to create a new VHD looks like (in its most minimal form)

```
create vdisk file=<filename> maximum=<size in megabytes>
```

For example, to create a 200MB VHD named *e:\test.vhd*, you’d type

```
create vdisk file="e:\test.vhd" maximum=200
```

That command would immediately create a 200MB file structured as a VHD. Notice that the parameter that sets a VHD’s size is *maximum=* rather than *size=*. This syntax drives me crazy. I can’t seem to break

myself of the habit of typing *size=*. But there’s actually a reason for using the *maximum=* parameter: expandable VHDs.

Immediately allocating that 200MB for *test.vhd* probably makes perfect sense because 200MB isn’t very big. For larger VHDs, however, you might not want to have Diskpart immediately allocate all the VHD’s space (for reasons I’ll explain in a moment). Instead of immediately allocating all the hard disk space that the VHD might ever need, you can allocate only a small amount of space on the actual hard disk, growing the VHD’s space only when necessary in the future. You do that by adding *type=expandable* to the Create Vdisk command:

```
create vdisk file=e:\test2.vhd maximum=200 type=expandable
```

Running that command instead of the first causes Diskpart to complete its task considerably faster, and it creates a VHD that initially takes up only about 2,500 bytes on the hard disk. (The *maximum=200* command makes a bit more sense now.) By the way, when you’re creating a fixed-size VHD, you can add the *type=fixed* option to the Create Vdisk command, although I’m not sure why you’d want to do the extra typing.

Fixed or expandable, which way to go? Fixed VHDs can be faster because all the time necessary to allocate the VHD’s disk space happens when you create it. Expandable VHDs haven’t allocated their space up front, so when you *do* need that extra space, the application writing to the VHD often must wait for the OS to obtain more space for an expandable VHD, thus slowing down the system—perhaps unacceptably. That being said, transporting a 20GB VHD over the web or on a USB stick is much easier to do if that 20GB VHD is expandable and hasn’t yet used more than a gigabyte; a fixed-size VHD is *always* 20GB, no matter how much of its space has actually been used. Expandable VHDs have another advantage in that they can be *compacted*—shrunk to the smallest size possible. Diskpart can’t reduce a fixed-size VHD.

Now you know how to use Diskpart to create a virtual hard disk, but that VHD is no good unless you take a few more important steps. I’ll guide you through those steps next month. 

InstantDoc ID 103685

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Mastering Windows Server 2008 R2* (Sybex). He writes and speaks around the world about Windows networking.

Microsoft VHD Test Drive Program

Today's IT staff has fewer people and smaller budgets than ever before. Yet businesses must evaluate and deploy new software solutions to remain competitive. The challenge to IT is streamlining that evaluation process despite having less equipment and time for testing. Because the cost of evaluation errors is high—possibly resulting in failed deployments or expensive rework—IT managers must take care to not reduce the benefit of their software evaluation and recommendations.

Evaluating new software solutions often requires complex installation, configuration, and integration that can be time consuming, especially if the evaluator is unfamiliar with the software. Fortunately, the Microsoft® Virtual Hard Drive (VHD) Test Drive Program can make even this arduous task much simpler by providing a Virtual Machine (VM) containing a complete evaluation environment that includes Windows Server® and all services and applications pre-configured.

associated applications, portable to any hardware platform running Microsoft Hyper-V™¹.

Hyper-V supports multiple simultaneous VMs, which can include both server and client operating systems. Thus, you can run multiple VHD Test Drive Images on a single virtualization host. Every VHD Test Drive Image is fully configured and ready to use, eliminating setup complexities, misconfiguration, and other errors (Figure 1).

In addition to rapid deployment, the VHD Test Drive Program can further streamline the evaluation process by leveraging the power of Hyper-V. Hyper-V offers the ability to snapshot the state of the VM so you can easily roll-back to a previous point in time. Virtual networking allows for a multi-tiered environment without the need for multiple physical network cards or expensive networking hardware. Abstraction from the physical hardware allows the evaluator to easily adjust VM resource settings such as CPU, memory, disk drives, and network cards.

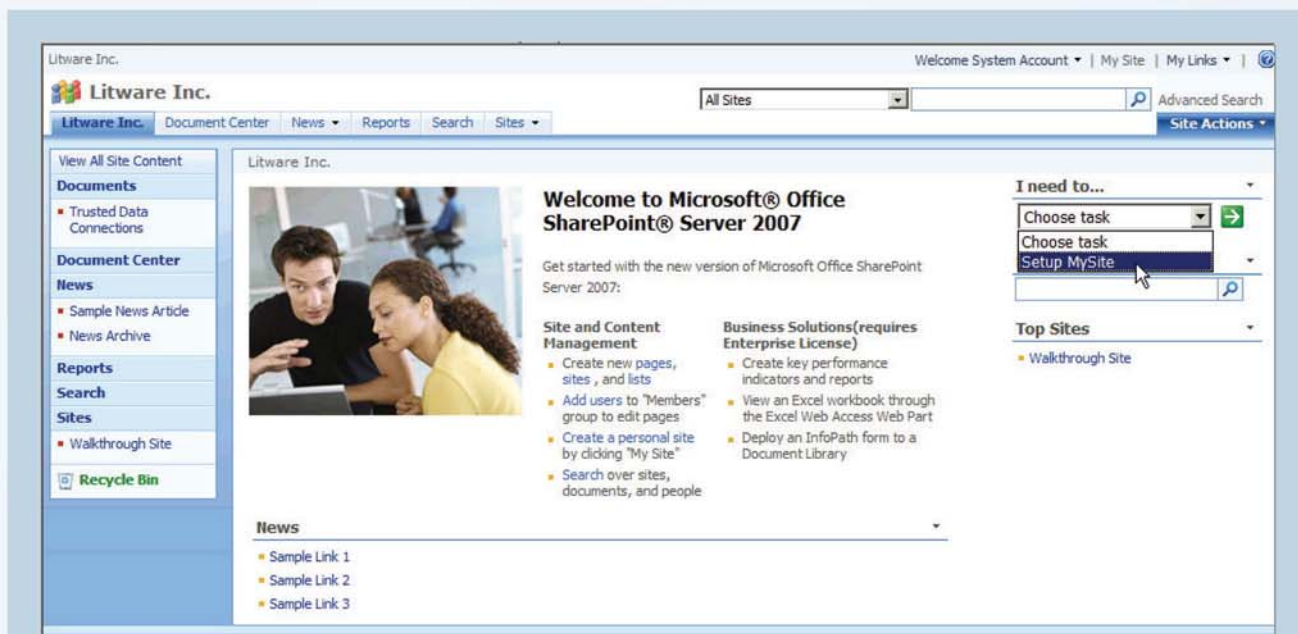


Figure 1: VHD Test Drive Images are ready to boot and fully configured for immediate use

The VHD Test Drive Program is a boon to harried IT managers and technicians, enabling them to quickly evaluate Windows-based software products. No longer is time lost installing and configuring applications and operating system components from scratch. Best of all, because VHD Test Drive Images are free, anyone can rapidly conduct an evaluation before committing to a solution or spending a dime on software.

This lets evaluators spend more time in the evaluation process, avoiding potentially costly deployment errors. Best of all, because VHD Test Drive Images are free, anyone can conduct an evaluation without spending a dime on software.

VHDs: What They Are and How They're Used

A VHD Test Drive Image is a VM that can be downloaded from the Internet or distributed via DVD, USB thumb drive, or other generic media. The VHD file itself is Microsoft's virtual hard disk format. A VHD Image is a hardware-independent encapsulation of a fully operational operating system and

Microsoft lists VHD Images for both its own products and partner products at the VHD Test Drive portal (<http://www.microsoft.com/vhd>). Microsoft-created VHD Test Drive Images include operating systems such as Windows Server 2008 R2 Enterprise Edition, productivity applications such as Microsoft Office SharePoint® 2007, and release candidate products such as Visual Studio® Lab Management 2010 RC. Partners such as Citrix, DataCore, and Prism Microsystems offer VHD Test Drive Images showcasing their technologies and solutions. In addition, new VHDs are being added constantly.

Runtime Requirements

VHD Test Drive Images are free and operate for a fixed time period of 30, 60, or 180 days, depending on the Windows Server version contained in the Image. A computer capable of running Hyper-V is required. In addition, the computer must have enough available resources for the VHD

¹VHD Test Drive Images execute on either Windows Server 2008 w/ Hyper-V or the no-charge Microsoft Hyper-V Server 2008 (or the R2 versions of either of these)

Test Drive Image itself (varies based on Image).

The Hyper-V virtualization platform is required to run VHD Test Drive Images. Hyper-V is available in the following products:

- Windows Server 2008 w/ Hyper-V
- Windows Server 2008 R2
- Microsoft Hyper-V Server 2008
- Microsoft Hyper-V Server 2008 R2

Both Microsoft Hyper-V Server 2008 and Microsoft Hyper-V Server 2008 R2 are free, stand-alone virtualization platforms. Some older VHD Test Drive Images were designed to be run on Virtual Server 2005, an early Microsoft virtualization product. However, these Images can be converted to run on Hyper-V.

VHD Walkthrough

Using a VHD Test Drive Image is a straightforward procedure that takes just a few clicks and keystrokes. The following is a sample procedure for running a VHD Test Drive Image containing Windows Server 2008 and Exchange Server 2007:

- Download the VHD Test Drive Image, or copy from its distribution media to the Hyper-V host computer.
- Open the VHD readme file, which specifies the memory requirements, networking requirements, and the VM Administrator password. In Hyper-V manager, create a new VM and attach the Test Drive VHD provided.
- Start and connect to the VM to monitor boot-up. When prompted, log into the VM using the credentials supplied in the readme file.
- If the VM requires automatic updates, it will install them automatically, which might require a reboot.
- After automatic updates, the VM is ready to use. Launch the Exchange Management Console from the Start menu and begin evaluating (Figure 2).

Frequently Asked Questions

The following are some frequently asked questions and answers about the VHD Test Drive Program.

- Q.** Can a VHD Test Drive Image be converted to production use by purchasing a license for the products it contains?
- A.** No. VHD Test Drive Images are designed for evaluation, testing, training, and demo purposes only.

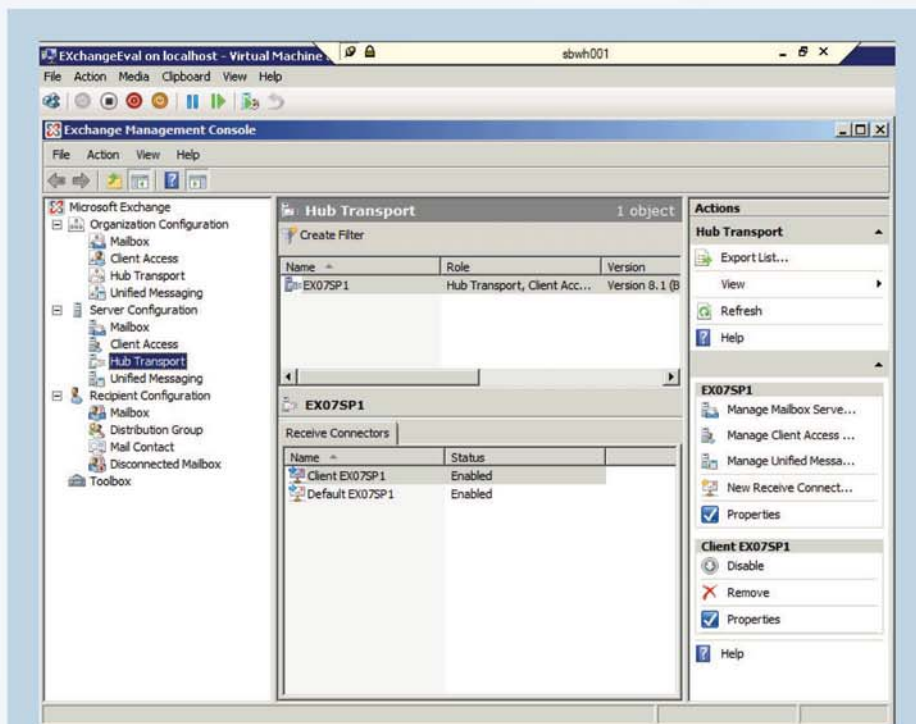


Figure 2: Exchange Management Console from VHD Test Drive for Exchange 2007

- Q.** Can VHD Test Drives be operated in a High Availability (HA) configuration?
- A.** Yes, by enabling iSCSI clustering between multiple VMs on a single host. Although this is not a practical HA environment for production purposes, it fully demonstrates all HA configuration and recovery processes.
- Q.** Is the VHD format open? Can anyone write tools that employ it?
- A.** Yes, the VHD format is fully public under Microsoft's Open Specification Promise program, which discloses all details of the VHD format.
- Q.** How long is the VHD evaluation period?
- A.** The evaluation period is 30, 60, or 180 days, and matches the evaluation period for the Windows Server operating system contained in the VHD Test Drive Image. This is 30 days for Windows Server 2003 R2, 60 days for Windows Server 2008, and 180 days for Windows Server 2008 R2.
- Q.** Are localized versions of VHDs available, or can VHDs be localized after startup?
- A.** VHD Test Drive Images are currently only in English.

Related Links

See the following resources for further information:

- Microsoft VHD Test Drive home page (<http://www.microsoft.com/vhd>)
- Hyper-V Getting Started Guide ([http://technet.microsoft.com/en-us/library/ee344828\(W5.10\).aspx](http://technet.microsoft.com/en-us/library/ee344828(W5.10).aspx))
- Complete list of current Microsoft VHDs by product (<http://technet.microsoft.com/en-us/bb738372.aspx>)
- Microsoft VHD FAQ (<http://technet.microsoft.com/en-us/bb738381.aspx>)
- VHD Image format specification (<http://technet.microsoft.com/en-us/virtualserver/bb676673.aspx>)
- Microsoft Open Specification Promise (<http://www.microsoft.com/Interop/osp/default.mspx>)

Yet Another 10 Free Tools for System Administrators

Audit Active Directory and file servers, detect inactive users, block USB devices, and more – for free

The following freeware tools by Windows IT Pro Community Choice Awards finalist NetWrix Corporation can save you a lot of time and make your network more efficient – at absolutely no cost. Some of these tools have advanced commercial versions with additional features, but none of them will expire and stop working when you urgently need them.

10. Disk Space Monitor (MS TechNet Magazine Sep'09: www.tinyurl.com/z2si83) — Even with today's terabyte-large hard drives, server disk space tends to run out quickly and unexpectedly. This simple monitoring tool will send you daily reports regarding all servers that are running low on disk space, below the configurable threshold. Download link: www.tinyurl.com/y5b6g8s

9. Bulk Password Reset (reviewed by SoftPedia: www.tinyurl.com/bdj483) — While most companies have strong password policies for their employees, one critical issue is still neglected: local Administrator passwords on all servers are usually managed in a “set and forget” fashion, sometimes using some “well-known” passwords, opening a major surface for security attacks. The Bulk Password Reset tool quickly resets local account passwords on all servers at once, making them more secure. Download link: www.tinyurl.com/fevgs9

8. Windows Service Monitor (WindowsReference.com: www.tinyurl.com/829287) — This very simple monitoring tool alerts you when some Windows service accidentally stops on one of your servers. The tool also detects services that fail to start at boot time, which sometimes happens, for example, with Exchange Server. Download link: www.tinyurl.com/yj2n7lz

7. VMware Change Reporter (TechTarget/SearchVirtualDesktop: www.tinyurl.com/8fg283x) — If you don't know what is being changed by your colleagues in the VMware infrastructure, it's very easy to get lost and miss changes that can affect the things for which you are responsible. This tool tracks and reports configuration changes in VMware Virtual Center settings and permissions. Download link: www.tinyurl.com/7fhs3h

6. Active Directory Object Restore Wizard (4sysops.com: www.tinyurl.com/brc827, Windows IT Pro Apr'10: InstantDoc ID 103641) — This tool can save the day if someone accidentally (or intentionally) deleted a bunch of Active Directory objects. It provides granular object-level and even attribute-level restore capabilities to quickly rollback unwanted changes (e.g., mistakenly deleted users, modified group memberships, etc). Download link: www.tinyurl.com/sghw82

5. File Server Change Reporter (4sysops.com: www.tinyurl.com/8g83d9) — This tool enhances the line of auditing tools; this one for file servers. File Server Change Reporter detects changes in files, folders, permissions, tracks deleted, and newly-created files, and sends daily summary reports. This is a very useful tool to detect mistakenly-deleted files and recover from backup or to see if someone changes some important files. Download link: www.tinyurl.com/scx3k9

4. Inactive Users Tracker (MS TechNet Magazine May'08: www.tinyurl.com/v348k9) — This feature tracks down inactive user accounts (e.g., terminated employees) so you can easily disable them, or even remove them entirely, to eliminate potential security holes. The tool sends reports on a regular schedule, showing what accounts have been inactive for a configurable period of time (e.g., 2 months). Download link: www.tinyurl.com/ng3u8s

3. Password Expiration Notifier (Redmond Magazine Feb'09, 4sysops: www.tinyurl.com/ard5n2) — This tool will automatically remind users to change passwords before they expire to keep you safe from password reset calls. It works nicely for users who don't log on interactively and, thus, never receive standard password change reminders at log on time (e.g., VPN and OWA users). Download link: www.tinyurl.com/uhc9a2

2. USB Blocker (Windows IT Pro Nov'09: InstantDoc ID 102860) — Users bring tons of consumer devices: flash drives, MP3 players, cell phones, etc., into the office and this aptly-named tool can block them with a couple of mouse clicks to prevent the spread of a virus and to restrict the take-out of confidential information. The product is integrated with Active Directory and is very easy to use. Download link: www.tinyurl.com/dsuf9e

1. Active Directory Change Reporter (Windows IT Pro Sep'09: InstantDoc ID 102446, Windows IT Pro Jan'09: InstantDoc ID 100593, TechTarget: www.tinyurl.com/72fgw2) — This is a simple auditing tool to keep tabs on what's going on inside Active Directory. The tool tracks changes to users, groups, OUs, and other types of AD objects, and sends summary reports with full lists of what was changed and how it was changed. In addition, it has a nice “rollback” feature that helps rollback unwanted changes (including deletions) very quickly. Download link: www.tinyurl.com/3k7vhd



"Although PsTools is a great collection of super-useful utilities, Disk2vhd is my new favorite tool."

Windows Sysinternals Tools

Find utilities to help you reveal rootkits, track down and terminate runaway processes, and remove unwanted programs from system start up

Sysinternals utilities have long been the administrator's best friend. Sysinternals was created in 1996 by Mark Russinovich and Bryce Cogswell, who gained notoriety for the powerful and practical Windows utilities they created. The Sysinternals toolset hasn't stagnated since Microsoft acquired it back in 2006. The company has continued to release new tools and improve existing ones. If you're new to Windows administration and haven't seen these utilities, you'll be blown away. Even if you have seen them, you might be surprised at many of the new tools and features that have been added. In this column, I'll share my favorite Sysinternals tools.

a program using a different user ID and password. You can get Shell-Runas at technet.microsoft.com/sysinternals/cc300361.aspx.

5 TCPView for Windows—TCPView gives you important information about what's happening beneath the surface of your Windows systems by showing all your open TCP and UDP connections. It lists the process name that the local port used and the remote address the process is connected to. You can get TCPView at technet.microsoft.com/sysinternals/bb897437.aspx.

4 Process Explorer—Process Explorer is a great tool for tracking down runaway programs and programs with memory leaks. Process Explorer shows you all the running processes on your system and lets you see the DLLs that are loaded as well as the CPU and memory utilization of each process. You can get Process Explorer from technet.microsoft.com/sysinternals/bb896653.aspx.

3 Autoruns for Windows—Discovering and optimizing the programs that run automatically when your system boots up is one of the best ways to improve your system performance. Autoruns displays all the registry and file locations that enable applications to run at boot and gives you the information you need to intelligently delete unwanted autostarting programs. Autoruns is at technet.microsoft.com/sysinternals/bb963902.aspx.

2 PsTools—The PsTools suite is a collection of 13 command-line tools that perform a number of useful tasks. For instance, PsExec executes processes on remote computers, and PsList displays information about running processes. PsKill terminates a process, PsLoggedOn shows all the local logins, and PsUptime shows the time since the last reboot. The PsTools suite is at technet.microsoft.com/sysinternals/bb896649.aspx.

1 Disk2vhd—Although PsTools is a great collection of super-useful utilities, Disk2vhd is my new favorite tool. Disk2vhd is a physical-to-virtual (P2V) disk-conversion utility. Unlike some P2V tools, Disk2vhd uses volume snapshots to allow it to copy any disk volume—including the one running Disk2vhd. Disk2vhd is at technet.microsoft.com/sysinternals/ee656415.aspx. 

InstantDoc ID 104650

MICHAEL OTEY (motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

10 RootkitRevealer—Rootkits are a type of malware designed to hide their presence from antivirus and antispysware solutions. Rootkits often work by intercepting and changing system API calls. RootkitRevealer runs as a randomly named service and detects rootkits by comparing the results of Windows API calls with the contents of the system's file structures. You can get RootkitRevealer at technet.microsoft.com/sysinternals/bb897445.aspx.

9 ZoomIt—ZoomIt is a favorite of mine for doing presentations. ZoomIt magnifies portions of the screen, which really helps you to draw attention to important points. ZoomIt also lets you create basic annotations on the screen. You can get ZoomIt at technet.microsoft.com/sysinternals/bb897434.aspx.

8 LogonSessions—This command-line utility shows you all the sessions that are currently logged on to your Windows system. It shows the username along with logon type, such as Service, Network, or Interactive. You can download LogonSessions from technet.microsoft.com/sysinternals/bb896769.aspx.

7 ShareEnum—Keeping your organization's file shares under control can be a challenge—particularly when end users and departments create their own shares, leaving you with lots of unused, obsolete shares on your network. ShareEnum can help you control the proliferation of file shares by listing all the available shares on your network as well as their basic security information. ShareEnum is available at technet.microsoft.com/sysinternals/bb897442.aspx.

6 ShellRunas—There are times when you want to run certain programs under a different set of logon credentials but you don't want to have to log off, then log back on again. ShellRunas adds a context menu option to Windows Explorer that lets you start

Making IT simple and easy
www.eventsentry.com

It's time  for more
uptime

Get a free AutoAdministrator license
after your 30-day trial of EventSentry:

www.eventsentry.com/AAM5

Limited time offer, restrictions apply.

**AWARD-WINNING EVENT LOG MONITORING & CONSOLIDATION,
SYSTEM HEALTH, ENVIRONMENT AND NETWORK MONITORING SUITE.**

EVENT  SENTRY

© Copyright 2010 NETKUS.NET Inc. All Rights Reserved. EventSentry is a registered trademark of NETKUS.NET Inc. in the United States and/or other countries.
All other trademarks are the property of their respective owners.



“Plan ahead of time where your zone information will be stored in AD before you configure it.”

Chasing the DNS Zone-Location Problem

Learn how to avoid or correct zone-replication conflicts on AD-integrated DNS servers

When you use Active Directory (AD)-integrated DNS servers and zones on Windows Server 2003 and later, an individual DNS zone's data can be stored in one of three locations in Active Directory. Zone Data can be replicated to 1) every domain controller (DC) in the domain, 2) every DNS server in the domain, or 3) every DNS server in the forest. A problem can occur when a single DNS zone is stored in more than one location and replication is attempted. I'll briefly discuss DNS zone replication, then show you an example DNS zone-location problem and steps you can take to solve it.

DNS Zone-Replication Settings

You configure DNS zone-replication settings using the Microsoft Management Console (MMC) DNS snap-in (Start, Administrative Tools, DNS). We'll walk through zone-replication setup using the example town.local primary zone. In the DNS console under Forward Lookup Zones, right-click the town.local zone, then click Properties, and the domain.local Properties (in this example, town.local) dialog box will be displayed. On the General Tab you'll see two options: Type, which is set to Active Directory-Integrated, and Replication (i.e., where the zones are kept in AD), which is set to *All DNS servers in this domain*. Clicking Change takes you to the Change Zone Replication Scope dialog box, in which three of the four options are available to store DNS zone information:

- To all DNS servers in this forest: town.local
- To all DNS servers in this domain: town.local
- To all domain controllers in this domain (for Windows 2000 compatibility): town.local
- To all domain controllers in the scope of this directory partition (grayed out)

I strongly recommend that you plan ahead of time where your zone information will be stored in AD before you configure it. The _msdcs.domain.local zone should be stored in the ForestDNSZones application partition. Each DC will register a GUID CNMANE record in the ForestDNSZones, and this information should be replicated to every DNS server in the forest, not just the domain. Other forward lookup zones and reverse lookup zones can be stored in ForestDNSZones, but to stay consistent and in line with an inverted DNS tree topology, where label hierarchy goes from top-level label

to a period-delineated multiple-label hierarchy (as outlined in the IETF RFC 1033 and RFC 1034), store the other forward and reverse lookup zones in DomainDNSZones within the Windows Server 2008/Windows 2003 application partition.

Zone-Location Problem

Now we'll look at how a problem might occur when zone settings are changed. Let's say you decided to place _msdcs.domain.local in the ForestDNSZones within the application partition and the forward lookup zone town.local and reverse lookup zone 1.268.192.in-addr.arpa in the DomainDNSZones partition. A couple of months go by, and DNS name resolution within your AD environment has been working like a champ.

But at this point, someone with enterprise administrator rights makes changes to the environment that affect the location of the DNS zones. The admin created a new DC, installed DNS, and allowed replication to pull ForestDNSZones and DomainDNSZones residing in the application partition over from a DNS server already in the domain environment. After a few weeks, the enterprise administrator returned to this DC/DNS server and changed the DNS zone town.local to reside within ForestDNSZones—instead of DomainDNSZones. However, time was needed for the _msdcs.domain.local zone to be removed from the other DNSDomainZones partition on the other DC/DNS servers and for town.local to be placed in ForestDNSZones by AD replication. The EventID 4521 and EventID 4011 errors occur, indicating that a problem is occurring with DNS A, PTR, and SRV registration. Furthermore, on one of the DNS servers, no town.local zone is displaying in the DNS console. Users are complaining that DNS resolution is not successful.

Possible Solutions

There are a couple of possible solutions for this problem. The first is the best-case scenario: Simply wait a bit longer for replication to finish. You can check on replication status by using the command `repadmin /showreps` or `repadmin /showrepl servername.town.local`. Note that you can queue up a forced replication by drilling down to the server object and the NTDS object in the MMC AD Sites and Services snap-in (I'll explain how to do this shortly).

If allowing replication to finish doesn't solve the problem, your next step is to use ADSI Edit to view the three locations in

■ WHAT WOULD MICROSOFT SUPPORT DO?

AD where the zone information can be stored—that is, to view ForestDNSZones and DomainDNSZones in the application partition and domain naming context (Windows 2000 storage location). For details on how to do this, see the Microsoft article “Event ID 4515 is logged in the DNS Server log in Windows Server 2003” at support.microsoft.com/kb/867464.

You want to determine where the town.local zone is located. Is town.local located in two different storage locations—say in ForestDNSZones and in DomainDNSZones? Or is town.local showing up in the ForestDNSZones on one Server 2008 DC/DNS server and in DomainDNSZones on another Server 2008 DC/DNS server?

Back in the earlier days of Windows 2003, Microsoft documented an issue in dns.exe regarding conflicts caused by a Microsoft DNS container being created prior to full replication of the application partition (see support.microsoft.com/kb/836534). Dns.exe 5.2.3790.125 and later versions solved this problem. Figure 1 shows what this type of conflict on a Server 2008 server might look like when observed through ADSI Edit.

The presence of a CNF (conflict) object indicates the existence of a conflict. In Figure 1, you can see that DC=town.local resides in both the ForestDNSZones partition and the DomainDNSZones partition. In DomainDNSZones, notice the object DC=.InProgress-57548AC124357A8-town.local located

under DC=domaindnszones,dc=town,dc=local, as well as the object CN=MicrosoftDNS0CNF54ce21bc-81e8-5af5-d112ebc8115, which indicates the conflict.

To remedy the conflict, first take a quick view of the zone information stored in the MicrosoftDNS0CNF object. Under this CNF object, view the contents of the town.local and 1.168.192.in-addr.arpa objects and compare with the .InProgress and town.local objects located under MicrosoftDNS. If the CNF object under DomainDNSZones contains all the record objects needed, and the DC=town.local object under ForestDNSZones contains only a few record objects, then do the steps in either Option 1 or Option 2, as follows:

Option 1

1. Make sure that you have a previous successful full system state backup of the DC available, so that if necessary, the zone town.local can be retrieved using a restore in Active Directory Restore mode.

2. Under domaindnszones.town.local, delete the object container CN=MicrosoftDNS. Note: Instead of deleting, an alternative, more precautionary step would be to rename the object container to something like CN=MicrosoftDNS-BackupDateTime, and then delete it after you’ve performed step 5—after verifying that DNS is working for the zone and DNS zone replication is successful.

3. Then, under domaindnszones.town.local, rename CN=MicrosoftDNS0CNF54ce21bc-81e8-5af5-d112ebc8115 to CN=MicrosoftDNS.

4. Force replication by using the AD Sites and Services snap-in or by using this syntax: repadmin /replicate Server4-W2K8.town.local Server3-W2K.town.local dc=town,dc=local.

5. Check replication status by issuing the command repadmin /showrepl Server3-W2K.town.local.

Option 2

Get your system state backup and restore the town.local zone from a previously successful backup. Any server resource records that are not on the town.local zone backup can be registered by pointing the unregistered server to the DNS server. Then from the command line issue the following commands, in sequence. (Make sure each command returns successfully before executing the next command.)

```
ipconfig registerdns
net stop netlogon && netstart Netlogon
net stop dns && net start dns
```

Know Where Your Zones Are

Always make sure you know where you intend to store your DNS zone information. Remember that the _msdcs.domain.local zone should be in ForestDNSZones within the application partition, and be sure to place forward and reverse lookup zones in DomainDNSZones within the application partition. Always have a valid system state backup that includes your DNS zones, just in case. You can use ADSI Edit to view where zone information is stored in AD. Become familiar with your DNS environment, and be cognizant of your DNS hierarchy and how your DNS servers are configured.

InstantDoc ID 104674

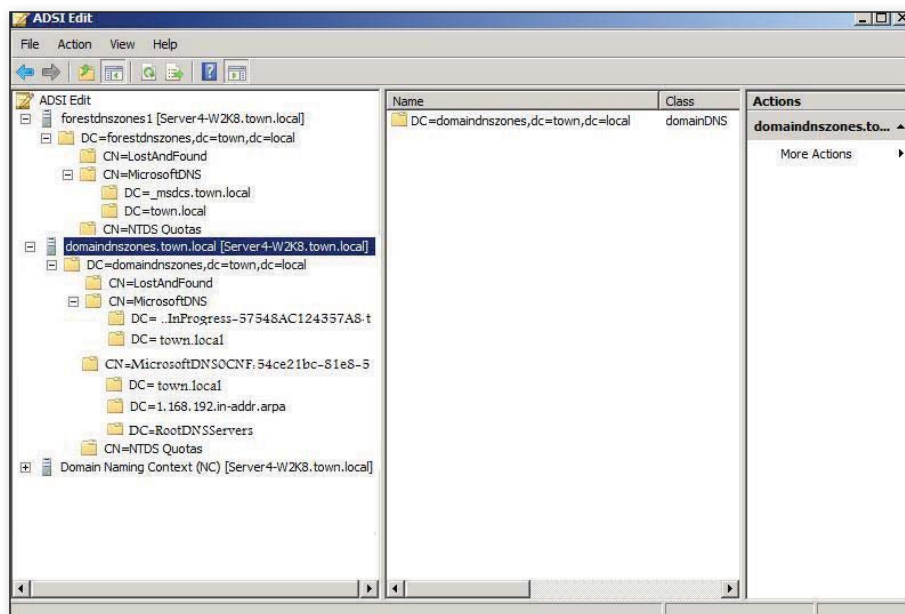


Figure 1: Viewing information about town.local zone in ADSI Edit

BOYD GERBER (boydg@microsoft.com) is a support escalation engineer with Microsoft Networking Escalation. His DNS industry experience is with DNS support and DNS development teams. He has a graduate degree in software engineering from the University of Texas at Austin.

■ Spiceworks
■ Internet Explorer

■ PowerShell
■ Exchange Server

READER TO READER

Tool Time: Inventory, Monitor, and Manage Networks with Spiceworks

When I was reading the web-exclusive sidebar “The Reader to Reader ‘Tool Time’ Reference” (www.windowstipro.com, InstantDoc ID 102777), I noticed that Spiceworks IT Desktop (www.spiceworks.com) wasn’t listed. This free application is for inventorying, monitoring, and managing networks as well as running a Help desk. I’m the administrator of two networks, and I’ve been using Spiceworks on them for several months. I started with version 4.1, but have since upgraded to version 4.5. (The upgrade process was quite painless.)

The tools in Spiceworks are fantastic, especially considering that it’s a freebie. I’ve found the tools in the Spiceworks Inventory section (see Figure 1) to be extremely handy, especially for creating asset lists. You can assign your devices (up to 1,000) to various built-in groups or custom groups you’ve created. For example, I have separate groups for our network switches, servers, printers, workstations, VoIP telephones, and so on.

You can use Spiceworks to keep tabs on what software, hotfixes, and services are installed on servers and workstations. By adding notes to devices, you can keep track of configuration changes or other pertinent information. Its reporting capabilities let

you run reports on various aspects of your network, even to the point of showing the number of pages your printers have printed. You can even have the system send you an email before each maintenance contract is set to expire so

that you can keep your maintenance contracts up-to-date.

If you have Wake on LAN (WOL) set on your devices, you can wake them up with this system. For example, if you need to roll out an update but a few users forgot to leave their workstations

running, you can power them up—very handy if those workstations are on a subnet at a remote site.

To help users report IT problems, you can run an IT Help desk with Spiceworks. The Help desk integrates with your mail system. My company uses IBM Lotus Notes, but Microsoft Exchange is also fully supported.

If you have IT problems or questions, you can connect with peers in the Spiceworks Community from the Spiceworks UI. I can assure you that they’re very friendly and very helpful.

Be aware that Spiceworks includes ads. They’re all IT-related, so you don’t have to worry about inappropriate ads (e.g., ads for online dating websites) appearing. For the most part, I mentally filter them out, but on occasion, I’ve found some ads quite

useful. If the ads are a problem, you can subscribe to a version (Spiceworks MyWay) in which the ads are replaced with your company’s logo and messages. This version costs \$20 per month or \$220 per year.

If you’re looking for free software that can help you inventory, monitor, and manage your networks or run a Help desk, give Spiceworks a try. The tools it provides are very useful, and I’ve had no problems using it. You can download Spiceworks 4.5 from www.spiceworks.com/signup. There’s also an early beta version of Spiceworks 4.6 (community.spiceworks.com/topic/91073). This version includes new functions, one of which is the ability to inventory and manage VMware ESX and ESXi hosts.

—Stephen Lyons, IT manager,
GEA Pharma Systems AG
InstantDoc ID 103686



Stephen Lyons

How to Quickly Change the Default Language in Internet Explorer

I frequently use Microsoft Internet Explorer (IE) to browse the Internet from computers that use an OS language other than English. A lot of websites that have content in various languages choose to serve their pages in the OS’s language. Although this is a good default for the typical user, I personally find it annoying. Take, for example, Microsoft’s website. I almost always want to read Knowledge Base articles (and other content) in English. But www.microsoft.com serves them in the OS’s language, so I’m forced to use the web page’s translation option to request the content in English or change the URL by adding the characters *en-us* to it. And when the content isn’t available in the OS’s language, I get the mildly annoying message: *We were unable to locate this content in xx-xx. Here is the same content in en-US.*

Besides Microsoft, lots of other websites assume that you want to read content in the OS’s language, so I came up with a solution to this problem. When you install IE, it checks the OS’s language and sets it as



Figure 1: The Inventory section in Spiceworks

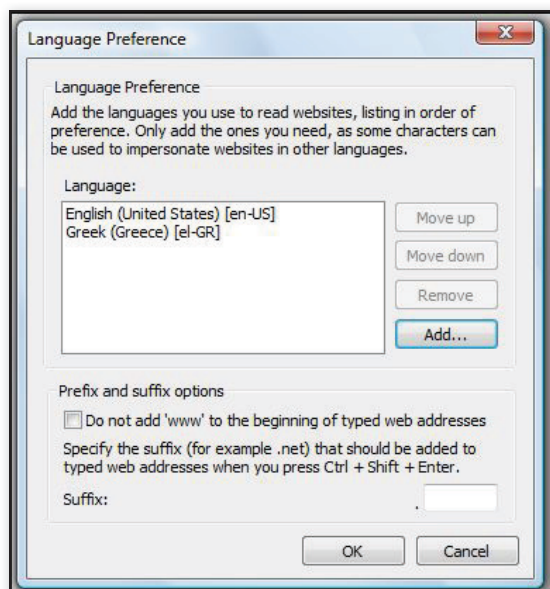


Figure 2: Changing the browser's default language

the browser's default language. Websites then check the browser's settings to detect which language to render their pages in. So, on the computer I'm going



Dimitrios Kalemis

to use for browsing the Internet, I change IE's default language. To do this, I select Internet Options on the Tools menu, then click the Languages button. This brings up the Language Preference dialog box that Figure 2

shows. If the *English (United States) [en-US]* entry isn't listed, I add it then move it to the top of the Language list box. If the *English (United States) [en-US]* entry is already listed but it's not at the top of the list box, I move it to the first position. In order for the change to take place, I then refresh IE. It's as simple as that.

Note that if you make this change to a computer other than your own, you might want to demote the *English (United States) [en-US]* entry when you're done browsing. To do so, just move the language that was previously at the top in that position again. That way, the next user won't have any surprises.

Besides putting the *English (United States) [en-US]* entry at the top of the Language list box, you can alternatively choose to put *English (United States)*

[en-US] as the only entry by removing all others or remove all the entries from the list box, leaving it empty. However, I have noticed that some sites don't serve English content when these alternative methods are used.

In the end, you should choose whichever method works best with the sites you visit most frequently. Just keep in mind that, depending on the website, these three methods might not always produce equivalent results.

—Dimitrios Kalemis,
systems engineer
InstantDoc ID 103684

Use PowerShell's Test-Path to Check Variables and Much More

Determining whether a variable exists before attempting to use it is helpful when writing scripts. However, if you look at the PowerShell cmdlets, you won't find a cmdlet devoted solely to this task. The reason is that PowerShell doesn't need one. It already has a more general cmdlet named `Test-Path` that does this as well as several other tasks.

Working with files and folders has always been a major part of administrative scripting, and checking whether a particular file or folder exists is frequently part of solutions. It's so common that PowerShell provides the `Test-Path` cmdlet to test whether a particular file or folder exists. For example, to see whether the `bootsect.bak` file exists on the root of the local C drive, you'd run the command

```
Test-Path -Path c:\bootsect.bak
```

This command returns *True* if `C:\bootsect.bak` exists and *False* if it doesn't. Similarly, to see whether the Windows folder exists on the root of the local C drive, you'd use the command

```
Test-Path -Path c:\windows
```

Files and folders aren't the only items that have paths in the PowerShell environment. The PowerShell drives expose all sorts of items, including variables, registry keys, functions, aliases, and certificates. All these items have paths, so you can use `Test-Path` to check for their existence.

To see all of the currently available drives in your system, you can run the `cmdlet`

```
Get-PSDrive
```

Figure 3 shows sample results. Notice the drives named `Variable` and `Env`. The `Variable` drive gives you a path you can use to access variables currently defined in the PowerShell environment. For example, if you want to test whether a variable named `ofs` exists, you'd use the command

```
Test-Path variable:\ofs
```

The `Env` drive contains environment variables inherited from the Windows shell environment. For example, to see whether the environment variable `%temp%` is defined, you'd run the command

```
Test-Path env:\temp
```

`Get-PSDrive` also exposes the `Function` drive and two registry drives. The `Function` drive lets you access PowerShell's functions the same way you would files and folders.



Alex K.
Angelopoulos

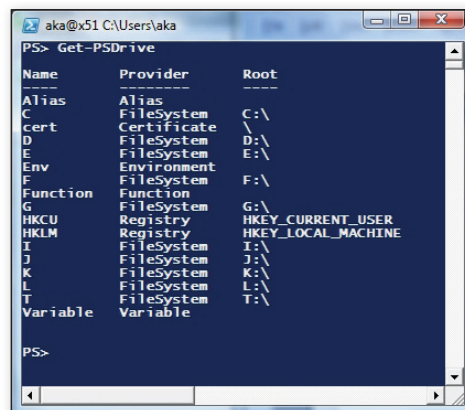


Figure 3: Sample output from `Get-PSDrive`

For example, to test for the built-in PowerShell function named *more*, you'd use

Test-Path Function:\more

The exposed registry drives are HKLM and HKCU. So, for example, to find out whether there's a registry key HKEY_LOCAL_MACHINE\Software, you'd run

Test-Path HKLM:\Software

The Test-Path cmdlet demonstrates the value behind PowerShell's "everything is a path" concept. Instead of having to use different tools to test for the existence of folders, files, registry keys, and other items like you do with VBScript and other traditional Windows-based scripting languages, you can simply use one tool (and one syntax) to test every item on any PowerShell drive. This lets you concentrate on using the results instead of worrying about how to get them.

—Alex K. Angelopoulos, IT consultant
InstantDoc ID 103682

How to Uninstall a Stubborn Exchange Server

Sometimes uninstalling a Microsoft Exchange server with the Control Panel's Add/Remove Programs applet isn't possible. The reasons vary, with one of them being that the Exchange server isn't able to communicate properly with the DCs. If you understand what occurs during an Exchange installation, you can manually undo the changes made by the Exchange setup process to remove an unwanted Exchange server.

Here are the changes that occur when you install Exchange server:

1. The Active Directory (AD) schema is extended. New class and attribute definitions are created.
2. The configuration information in AD is modified. Under the Configuration partition in the Services section, a new container named Microsoft Exchange is created. This container represents the Exchange organizational hierarchy.
3. New user groups are created in AD. For example, in Exchange Server 2003 and Exchange 2000 Server, two user groups—Exchange Domain Servers and Exchange Enterprise Servers—are created

in the domain's Users container. The Exchange servers in a domain are members of the Exchange Domain Servers group. The Exchange Domain Servers group is a member of the Exchange Enterprise Servers group. In Exchange Server 2010 and Exchange Server 2007, several new groups are created under a new organizational unit named Microsoft Exchange Security Groups, which resides in the root domain of the forest.

4. The server's registry is changed. The changes occur in two registry keys: HKLM\Software and HKLM\System\CurrentControlSet\Services.

5. A folder hierarchy for the Exchange installation files is created under a folder specified during installation.

If you want to manually uninstall an Exchange server, you must manually undo some of these changes:

1. You don't need to worry about the AD schema changes that the Exchange installation made. These changes can't be reversed because you can't delete schema objects and attributes. Even if you could, it wouldn't be a good idea. If you have multiple Exchange servers, the remaining servers need these schema objects and attributes. Plus, if you uninstall a lone Exchange server, the schema objects and attributes that remain won't cause any problems. In fact, if you should later decide to install Exchange again, it would take a shorter time because the schema have been already changed.
2. The server's configuration information in AD can be removed using the ADSI Edit console (ADSIEdit.msc). In Windows Server 2003 and Windows 2000 Server, this tool is one of the Support Tools, which aren't install by default. In Windows 2008, the ADSI Edit console is installed by default. To remove the configuration information, open the ADSI Edit console and navigate to Services\Microsoft Exchange\ExchangeOrgName\AdministrativeGroups\RelatedOrganizationGroup\Servers, where *ExchangeOrgName* is the name of your Exchange organization. After you locate the server you want to uninstall, simply delete it.

Alternatively, you can delete the Microsoft Exchange container altogether.



Murat Yildirimoglu

By doing this, you delete the Exchange organization's information in AD. However, be aware that removing a server this way isn't supported by Microsoft unless you're instructed to do so by its Customer Service and Support (CSS) staff. In addition, you run the risk of leaving semi-deleted objects or partially mail-enabled objects in AD.

This isn't important if you don't plan to install Exchange into a forest again, but it is important if you do, as you can run into problems. To mitigate these risks, I delete the Microsoft Exchange container after moving the mail-enabled objects to other servers or after deleting them.

3. You can delete the user groups related to the Exchange server, but this step isn't necessary. You should do it only if you want to undo all the changes.

4. You need to delete the following registry keys on the Exchange server:

- In Exchange 2010 and Exchange 2007, delete the HKLM\Software\Exchange and HKLM\Software\Exchange Server keys.
- In Exchange 2003 and Exchange 2000, delete the HKLM\Software\Exchange key.
- In the HKLM\System\CurrentControlSet\Services key, delete the keys that were created for the Exchange Server services. In Exchange 2010 and Exchange 2007, all the keys related to the Exchange Server services start with *MSEExchange* (e.g., MSEExchangeIS). In Exchange 2003 and Exchange 2000, most of the keys also start with *MSEExchange*. However, three keys have names that don't include this string. They are IMAP4Svc, POP3Svc, and RESvc.

5. You should delete the files under the root Exchange Server folder.

By following these steps, you can manually uninstall an Exchange server. I've done so successfully several times.

—Murat Yildirimoglu, MCSE and MCT

InstantDoc ID 103660

■ Event Log
■ Outlook
■ Office

■ Hyper-V
■ System Restore

ANSWERS TO YOUR QUESTIONS

Q: What are the different Windows Logon Types that can show up in the Windows event log?

A: Logon Types are logged in the Logon Type field of logon events (event IDs 528 and 540 for successful logons, and 529-537 and 539 for failed logons). Windows supports the following logon types and associated logon type values:

- 2: Interactive logon—This is used for a logon at the console of a computer. A type 2 logon is logged when you attempt to log on at a Windows computer's local keyboard and screen.
- 3: Network logon—This logon occurs when you access remote file shares or printers. Also, most logons to Internet Information Services (IIS) are classified as network logons, other than IIS logons that use the basic authentication protocol (those are logged as logon type 8).
- 4: Batch logon—This is used for scheduled tasks. When the Windows Scheduler service starts a scheduled task, it first creates a new logon session for the task, so that it can run in the security context of the account that was specified when the task was created.

- 5: Service logon—This is used for services and service accounts that log on to start a service. When a service starts, Windows first creates a logon session for the user account that is specified in the service configuration.
- 7: Unlock—This is used whenever you unlock your Windows machine.
- 8: Network clear text logon—This is used when you log on over a network and the password is sent in clear text. This happens, for example, when you use basic authentication to authenticate to an IIS server.
- 9: New credentials-based logon—This is used when you run an application using the RunAs command and specify the /netonly switch. When you start a program with RunAs using /netonly, the program starts in a new logon session that has the same local identity (this is the identity of the user you are currently logged on with), but uses different credentials (the ones specified in the runas command) for other network connections. Without /netonly, Windows runs the program on the local computer and on the network as the user specified in the runas command, and logs the logon event with type 2.
- 10: Remote Interactive logon—This is used for RDP-based applications like Terminal Services, Remote Desktop or Remote Assistance.
- 11: Cached Interactive logon—This is logged when users log on using cached credentials, which basically means that in the absence of a domain controller, you can still log on to your local machine using your domain credentials. Windows supports logon

Q: How can I find the Windows Server 2008 event IDs that correspond to Windows Server 2003 event IDs?

A: The event ID numbering scheme changed for Windows 7, Server 2008, and Windows Vista. You might need to figure out the corresponding IDs so that you can use them with your monitoring software.

To find the Server 2008 event ID that corresponds to a given Server 2003 event ID, use the following simple rule:

Server 2003 event ID + 4096 = Windows Server 2008 Event ID.

Exceptions to this rule are the Windows logon events:

- The successful logon events (event IDs 528 and 540) have been merged into a single event, 4624 (this is 528 + 4096).
- The failure logon events (event IDs 529 through 537 and 539) have been merged into a single event, 4625 (this is 529 + 4096).

—Jan De Clercq
InstantDoc ID 103570

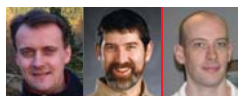
using cached credentials to ease the life of mobile users and users who are often disconnected.

—Jan De Clercq
InstantDoc ID 103572

Q: How can I customize my calendar day view in Outlook?

A: One of my clients runs a call center with many part-time people who work only a few days a week. This client showed me a little trick for presenting only certain days of the week in the calendar view.

When you select the Calendar view in Office Outlook 2003 or Outlook 2007, there is by default a small calendar on the top of the Navigation Pane, which resides on the left side of the main Outlook UI. When you click a day in that small



Jan De Clercq | jan.declercq@hp.com
William Lefkovich | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com

calendar, that day is then reflected in the main UI with the Day view. At this point, you can add individual, non-sequential days to the view. Hold the CTRL button down, and click other days in the small calendar in the navigation pane. You can also span different months by advancing the little calendar in the navigation pane and selecting other dates; remember to hold the CTRL key down. Outlook adds these days to the view sorted by time. Also, if you try this with multiple calendars open, all of the open calendars change to the Day view with the days you selected displayed.

This is just a local view of the calendar. Exporting the calendar to an .ics file using File, Save As does not retain this view nor does publishing the calendar to a web page. If you want to print this view and retain it, you must take a screen capture and print that instead.

—William Lefkovic
InstantDoc ID 103637

Q: How do I use date formulas in Outlook?

A: Sometimes when you create a new appointment or meeting request, you need to pause to figure out exactly what day the meeting should happen. Additionally, when you create a task, you might struggle with figuring out the actual calendar day that the task should be completed by.

Outlook offers some assistance with this task. The most obvious aid is the drop-down calendar right from the New Appointment form. This is the same for the New Meeting Request and New Task forms. Sometimes you want meetings to occur in a specified number of days or weeks. A less obvious aid in determining a specific meeting date can be found in the date field itself. Outlook recognizes terms we use for calendar units of time—hours, days, weeks, months, and years. If you need to set a task to be due 45 days from tomorrow, you can just enter “Tomorrow + 45” days in the Due Date field of the New Task form, and Outlook will perform the simple calculation. Press Tab and Outlook will show the new date.

This field recognizes several different combinations for these formulas. For

example, instead of “Tomorrow + 45 days,” you can just enter “+ 46 days.” A meeting intended for a month from Friday can be entered as “Friday + 1 month.” You can easily change the date of a task due in exactly one year by typing “+ 1 year.” You can further abbreviate the formula by using the first three letters only to assign a day (e.g., Mon). And you can use the first letter to abbreviate the unit of time. “Friday + 1 month” can be further shortened to “Fri + 1 m.”

Using these formulas is sometime easier than trying to count a number of days after a certain date to determine the date you need to enter in Outlook.

—William Lefkovic
InstantDoc ID 103638

Q: Can I use System Idle time to check how long my box has been running?

A: Sadly, no. The System Idle time reported in Task Manager is essentially the amount of time the CPU has been idle. In a busy box, this counter wouldn't be accurate, but it's even worse than that in a multi-core machine. Each core's time is considered, so if I have four idle cores, the System Idle time would increase four seconds each second. (Make sure you enable *Show processes from all users* if you can't see your System Idle time in Task Manager.)

In Figure 1, you can see Task Manager on my 16-core server (well, eight cores with Hyper-Threading). Task Manager shows a much longer System Idle time than my system really has—every second the System Idle time increases by 16 seconds (when the server is idle). As you can see, System Idle shows the server as being up for 53 days (1272 hours), but in

reality it had only been three days as of when I wrote this on Feb. 23.

—John Savill
InstantDoc ID 103662

Q: I have a command that I'm trying to automate that requires a key to be pressed. What can I do?

A: The easiest way to handle commands that require user input and don't support command line switches is to simply pipe the required character to the command. For example, if I need to press y, I could do the following:

```
cmd /c call ECHO Y | command.exe
```

—John Savill
InstantDoc ID 103669

Q: Can I replace the recovery environment provided with Windows 7 and Windows Server 2008 R2 with the Microsoft Diagnostic and Recovery Toolset (DART) environment?

A: When an OS has problems booting, it uses the recovery environment to resolve the issue. You can access this environment by pressing the F8 key before the Windows logo displays during boot and and selecting Repair your computer.

The recovery environment is stored in the file Winre.wim, which is found in the folder C:\Recovery\<GUID>. This folder is hidden and protected by default, so you'll need to enable Show hidden files, folders and drives and disable Hide protected operating system files in Explorer's folder options.

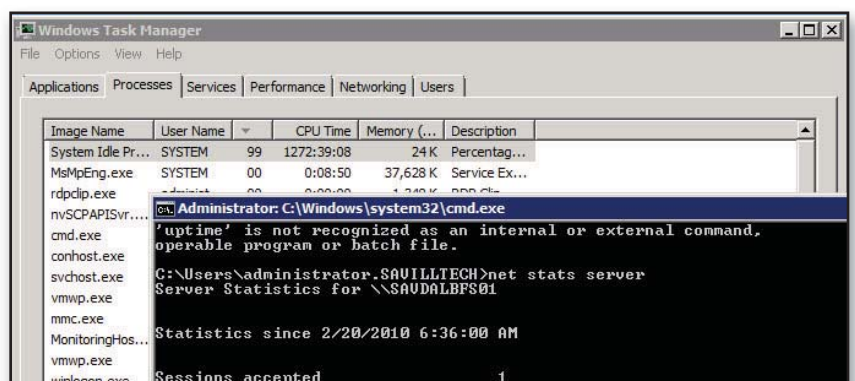


Figure 1: Task Manager on a multi-core system

■ ASK THE EXPERTS

You'll now see the Recovery folder at the root of the C: drive, but you won't have permission to navigate its contents. Select the properties of the folder and edit its security. Give yourself Full Control and click OK.

You can now navigate inside the folder, rename the Winre.wim to Winre.old_wim and copy in the DART sources\boot.wim from your DART CD, renaming it to Winre.wim. Now when you select Repair Your Computer, the recovery environment will have DART built-in.

Q: Can I migrate users to a Windows Server 2008 R2 domain with Active Directory Migration Tool (ADMT) 3.1?

A: ADMT 3.1 was designed to be used for the migration of Windows Server 2003 and Windows 2000 to Server 2008, Server 2003, and Windows 2000 domains. It's designed to be installed only on a Server 2008 server. ADMT 3.2 will support installation on Server 2008 R2 servers.

Microsoft has performed testing with ADMT 3.1 to a target of a Server 2008 R2 domain and do support the action, with a couple of gotchas you need to watch out for. They documented these in Knowledge Base article 976659.

—John Savill

InstantDoc ID 103564

Q: How can I extract a Microsoft Office service pack for enterprise deployment?

A: When you download an Office service pack, you typically get one big file. When we run this file on a client, it's extracted locally on the client then executed. This process can take a lot of disk space and slow down your installation. It's also very annoying if you're virtualizing applications and the service pack application generates a large cache of patches.

You can extract a service pack to a folder using the /extract switch. For example:

```
"D:\Software\Office 2007\en_2007_
microsoft_office_suite_service_
pack_2_x86.exe" /extract:"d:\
software\office 2007\sp2"
```

—John Savill

InstantDoc ID 103676

Q: Should I use System Restore on my virtual machines (VMs) that use dynamic disks?

A: This isn't an absolute rule, but system restore can lead to a significant amount of disk usage that will cause your dynamic disks to grow. I would recommend you disable System Restore for most VMs that are using dynamic hard disks. You can disable it on each VM, or for Windows 7 and Windows Server 2008 R2, you can use Group Policy. Go to Computer Configuration, Policies, Administrative Templates, System, System Restore, Turn off System Restore, as Figure 2 shows.

Ideally, you can apply this policy to a specific Organizational Unit that contains the VMs. Make sure you don't apply this Group Policy to machines that should still have System Restore protection.

—John Savill

InstantDoc ID 103672

Q: One of my Exchange Server 2010 servers has failed and I don't have a backup. What's the easiest way to recreate the server?

A: Exchange installs most of its configuration data in Active Directory (AD), so if you need to rebuild a failed Exchange server and don't have a good backup, you can actually tell the Exchange installation process to check with AD. It will pull down the old configuration information and use it, with the caveat that the new Exchange server must have the same name as the one it's replacing.

To use the recovery server mode, enter the command from a command prompt, with the Exchange media folder as the current location.

```
setup /m:RecoverServer
```

Note that this will perform an unattended installation of Exchange server. You must have installed all the prerequisites for the Exchange roles and enabled the required services per a normal Exchange 2010 installation.

Once the installation is complete, the server will have all the same roles as before. If the server was previously a mailbox server, you'll need to restore the

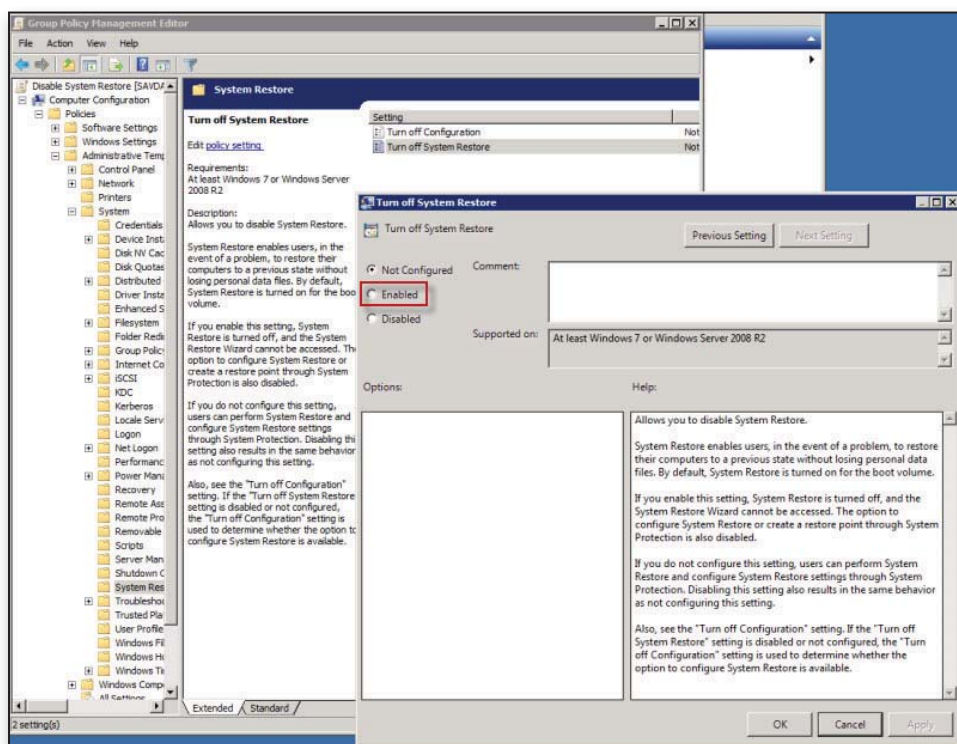


Figure 2: Turning Off System Restore

mailbox databases—mailbox database content isn't stored in AD!

—John Savill
InstantDoc ID 103560

Q: Are Database Availability Groups (DAGs) included in the standard edition of Exchange Server 2010?

A: Surprisingly, DAGs are available both in the standard and enterprise editions of Exchange 2010. However, you always need to install Exchange on the enterprise edition of Windows Server 2008 for failover cluster support.

Note that although you can do DAG with the standard edition of Exchange 2010, you'll be limited to five databases (the enterprise edition supports 100 databases), so the standard edition will only be useful for smaller environments.

Also note that you can mix standard and enterprise editions of Exchange 2010 in the same DAG. You could, potentially, use the standard edition to host the mailboxes for users at a remote site and then replicate them back to the central Exchange mailbox servers.

—John Savill
InstantDoc ID 103551

Q: How can I export and import calendar data with Microsoft Office Outlook 2010?

A: Outlook 2010 moves a number of features around, so it's not always obvious how to perform certain actions.

If you want to export data from Outlook, you need to click the File tab,

Open, then Import, as Figure 3 shows. Yes, Import, even though you want to export.

The Import and Export wizard will launch with *Export and Import options* showing. From here, you can select *Export to a file*, select the data to save, and choose where you want to save.

—John Savill
InstantDoc ID 103582

Q: How can I un-cluster a Hyper-V virtual machine (VM)?

A: If you made a VM highly available using failover clustering and now you want to make it a standalone VM again, the easiest way I've found is to export the VM to the desired location. Delete the virtual machine as a resource group from failover clustering, delete the VM from the Hyper-V snap-in, then import it back in.

Because you already exported the VM to the desired final location, there's no need to duplicate the files again when you perform the import. Select the *Move or restore the virtual machine (use the existing unique ID)* option and don't check the *Duplicate all files so the same virtual machine can be imported again*.

—John Savill
InstantDoc ID 103559

Q: Can I have a mix of Windows Server 2008 and Server 2008 R2 in my Exchange 2010 Database Availability Group (DAG)?

A: Exchange 2010 is supported on the 64-bit editions of both Server 2008 and Server 2008 R2, but you can't mix the OSs within a single DAG.

This limitation is because DAGs use Windows failover clustering behind the scenes, and failover clustering doesn't support a mix of Server 2008 and Server 2008 R2 nodes in the same cluster (because of differences in cluster implementation).

If you want a mix of Server 2008

and Server 2008 R2, you'll need to have multiple DAGs, each containing one version of Windows.

—John Savill
InstantDoc ID 103558

Q: How can I enable or disable a Windows role or feature with DISM?

A: You can use the /enable-feature switch with DISM to enable a feature or role on a Windows 7 or Windows Server 2008 R2 installation. For example, the command

```
dism /online /enable-  
feature:InkSupport
```

will enable ink support, as shown here.

```
Deployment Image Servicing and  
Management tool  
Version: 6.1.7600.16385
```

```
Image Version: 6.1.7600.16385
```

```
Enabling feature(s)  
[=====]  
100.0%  
=====]
```

```
The operation completed successfully.  
Restart Windows to complete this  
operation.
```

```
Do you want to restart the computer  
now (Y/N)? n
```

Similarly, you can use the /disable-feature option to disable a role/feature. You can get the name of the role or feature you want using DISM's /get-features and /online switches.

—John Savill
InstantDoc ID 103552

Q: Are there any domain or forest functional level restrictions when using Active Directory Migration Tool (ADMT) 3.1?

A: ADMT is fairly flexible. For the target domain, you can be running any domain or forest level above Windows 2000 native mode. There are no strict requirements about having to be at least Windows 2008 mode, for example.

—John Savill
InstantDoc ID 103563

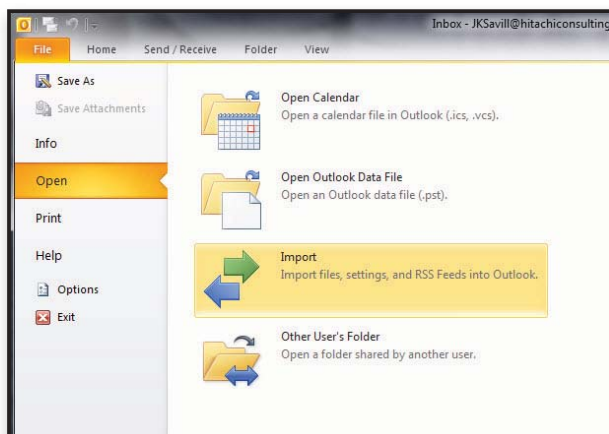


Figure 3: Exporting Outlook Data

Migrating from Exchange Server 2003 to Exchange Server 2010

A Small Organization Perspective

Learn from a real-world example

by Michael B. Smith

In this article, you'll learn how to migrate your Microsoft Exchange Server 2003 infrastructure (both your front-end and back-end servers) to Exchange Server 2010. I'll focus on the requirements of smaller organizations because the needs of larger organizations typically just scale up from there.

I was lucky enough that one of my partner companies, Clark Systems Support (www.clarksupport.com), allowed me to do their migration, and I based this article on that experience.

Exchange Deployment Assistant

Microsoft has recently released a new tool, the Exchange Server Deployment Assistant (EDA); it's available at technet.microsoft.com/exdeploy2010. Using a series of simple questions, the EDA prepares a customized set of instructions for a given scenario. As a broad overview of the steps to be accomplished for an Exchange migration, it's a good start. However, because the tool is designed to be generic, it tends to make some things that can be accomplished in a single step take three or more steps (such as a typical single-server installation of Exchange). It also completely misses some things, such as the requirement for installing the newly created legacy SSL certificate on legacy Exchange 2003 servers.

As you begin to do your own upgrades (hopefully in a test environment before your production environment), keep Microsoft's definitions in mind. Microsoft defines an *upgrade* as an increase in product version that can happen in place (that is, on the same server or workstation). A *migration* is when the new product is installed on another computer and information is moved to the new computer, with little or no impact to users. A *transition* occurs when information is exported from one version of a product and then imported into another installation of the product (whether it be the same or a later version).

Exchange hasn't provided an upgrade since Exchange 2003 (which could be installed on top of Exchange 2000). For both Exchange 2007 and Exchange 2010,

the new version has to be installed and configured, with user mailboxes (and other configuration items) then moved from the old servers to the new servers. This is considered a migration in Microsoft-speak.

Background

My partner company has the following configuration:

- Windows Server 2003 SP2 is running on all domain controllers (DCs).
- CLARK2K3 is the sole Exchange 2003 server. It's running Exchange 2003 SP2, with a few hotfixes. It's running Server 2003 SP2.
- CLARK2008 will be the new Exchange 2010 server. It's running Windows Server 2008 R2 with all current Microsoft updates.
- The NetBIOS name of the domain is CLARK. It's been around since Windows NT 4.0.
- The Active Directory (AD) is named clarksupport-hq.com.
- Both the forest functional level and the domain functional level are set to Windows 2000.
- The Exchange organization is named Clark.
- The original Exchange administrative group in the organization is named HQ.

As is common in smaller organizations, CLARK2K3 is the only server in the clarksupport-hq.com domain, and although it's not running Small Business Server (SBS), it's also a DC. For information about installing Exchange on a DC, see the sidebar, "Exchange on a Domain Controller."

Step 1: Exchange Prerequisites

Before you can install Exchange 2010, there are certain things that you must verify about your existing Exchange environment. The Exchange setup process checks these things too, but it's best that you verify them for yourself, so that when setup throws an error it doesn't come as a surprise.

Exchange must be in Native mode. You can't have any Exchange 2000 servers and all Exchange 2003 servers must be at SP2. You must also have KB937031 installed. To verify that Exchange is in Native mode, open Exchange System Manager (ESM), right-click the Exchange Organization name in the selection pane, and click properties. You'll

get a dialog box with the Operation mode displayed. If the organization isn't in Native mode, you'll have the option to change the mode of the organization in this dialog box. There are several prerequisites for upgrading an organization to Native mode, but they're outside the scope of this article. Refer to the Microsoft article "XADM: Preparing a Mixed Mode Organization for Conversion to Native Mode" (support.microsoft.com/kb/272314).

You can also use ESM to see the versions of the Exchange servers you have in your organization. If your ESM is configured to display Administrative Groups, expand the Administrative Groups node, then expand the node containing your historical administrative group (AG). Once you've prepared your environment to install either Exchange 2007 or Exchange 2010, you'll find a new AG named Exchange Administrative Group (FYDIBOHF23SPDLT). (For more information about FYDIBOHF23SPDLT and other special character sequences in Exchange 2007 and Exchange 2010, refer to bit.ly/cdprm2.) After you've expanded the proper AG, click the Servers node beneath it. All the Exchange 2000 and Exchange 2003 servers will be displayed in the results pane, including their versions. Version 6.0 is Exchange 2000 and version 6.5 is Exchange 2003.

Remember, you can't install Exchange 2010 if you have any Exchange 2000 servers remaining. If this display shows any, you'll need to remove them. Similarly, be sure all Exchange 2003 servers are at SP2.

Finally, on all your Exchange 2003 servers, install the hotfix from the Microsoft article, "Event ID 1036 is logged on an Exchange 2007 server that is running the CAS role when mobile devices connect to the Exchange 2007 server to access mailboxes on an Exchange 2003 backend server" (support.microsoft.com/kb/937031). Following the instructions in the article, enable Integrated Windows Authentication on the Microsoft-Exchange-ActiveSync directory.

Step 2: Active Directory Prerequisites

Exchange 2010 will make some fairly major changes to your AD during the installation process. But before that can be done, Exchange has certain requirements that must be met:

- The server holding the schema master flexible single master operator (FSMO) role must be running Server 2003 SP1 or higher.
- There must be at least one Global Catalog (GC) server that's running Server 2003 SP1 or higher installed in the site where Exchange will be installed.
- The AD forest must be at the Server 2003 forest functional level (FFL) or higher.
- The AD domain must be at the Server 2003 domain functional level (DFL) or higher.

To check the DFL, open the Microsoft Management Console (MMC) Active Directory Domains and Trusts snap-in, right-click the AD domain, and select Raise Domain Functional Level. (Don't worry; this is non-destructive at this time). If the dialog box that appears says your DFL isn't high enough, you'll need to raise the DFL to at least Windows Server 2003. To view the current FFL, right-click the line above the domain, which starts with Active Directory Domains and Trusts, and select Raise Forest Functional Level.

Exchange 2003 and Exchange 2010 both support you raising the DFL and FFL all the way up to Server 2008 R2. However, as long as you have Windows 2000 DCs in your environment, you won't be able to update the functional levels higher than Windows 2000. This necessitates you removing all Windows 2000 DCs from your environment prior to the installation of Exchange 2010. Similarly, as long as you have Server 2003 DCs in your environment, you won't be able to raise the levels beyond Server 2003. However, because that's what Exchange 2010 requires as a minimum, it will be sufficient for this need.

The specific considerations for upgrading your functional levels are beyond the scope of this article. Suffice it to say that for most small and medium businesses, there are few problems. For more information, refer to the Microsoft article at bit.ly/bWO6Y8.

The final AD prerequisite to consider is whether this Exchange server will be a DC (remembering the caveats expressed earlier). If so, now is the time to add the Active Directory Domain Controller Server Role to the computer and then execute `dcpromo.exe`.

Step 3: Preparing to Install Exchange

Now that the infrastructure has been prepared, you can get on with the actual work involved in installing Exchange 2010. There are many paths to success, but the one I present here is tested and known to work. As a reminder, Exchange 2010 *must* be installed on 64-bit hardware. There is no 32-bit version of the software available.

You can install Exchange 2010 on either Server 2008 SP2 or Server 2008 R2. I recommend you use Server 2008 R2. It will not only have a longer lifetime (per Microsoft's standard lifecycle policies), but it also has one less piece of software to download and install. If you're running Server 2008 SP2, you need to download and install Windows Management Framework from Microsoft support.microsoft.com/kb/968929.

If you have Exchange 2010 on a DVD, I recommend you create a location on disk and copy the DVD there. I'll use D:\Exchange2010 as the target for this purpose. If you downloaded Exchange in an executable or ISO format, extract the contents of the archive to that location.

Next, determine the most recent rollup available for Exchange, and place it into the Updates folder (D:\Exchange2010\Updates). The Exchange setup process will automatically apply the rollup during installation. At this writing, Rollup 1 is current and can be downloaded from Microsoft, but by the time you read this, additional rollups should be available. You can determine the most recent one by checking bit.ly/4vtBJo.

Next, open a command prompt (or a PowerShell session) and enter the following commands:

```
D:
Cd Exchange2010\scripts
ServerManagerCmd -ip Exchange-Typical.xml -restart
```

This command causes the various server roles and server features that Exchange requires to be installed and then executes a reboot. If you use ServerManagerCmd on Server 2008 R2, it will warn you that it is "deprecated and not guaranteed to be supported in future releases of Windows." However, it will work just fine for your needs. The other mechanisms for installing Exchange prerequisites (DISM

and Add-WindowsFeature) are much more complicated and confusing to use.

Go to microsoft.com/downloads, then search for and download "2007 Office System Converter: Microsoft Filter Pack," ensuring that you retrieve the x64 version—the name of the file is FilterPackx64.exe. Once it's downloaded, install the filter pack, which is used by the Exchange full-text search engine to search Office format documents.

The final preparation steps are somewhat dependent on how you've installed your Windows server and what other server roles and features have been installed. Therefore, if you get errors indicating that a step has already been completed, that's OK. Open a command prompt and execute the commands

```
sc config NetTcpPortSharing start= auto
net start NetTcpPortSharing
```

For the *sc config* command, the space following *start=* is required.

Step 4: Beginning the Installation

Exchange maintains extensive log files that record the steps taken during the installation process, located in C:\ExchangeSetupLogs. You'll be able to find a number of scripts and XML files that are created during installation, but the most important single file is named ExchangeSetup.log.

In larger environments, Exchange administrators, domain administrators, enterprise administrators, and schema administrators are often different people. In small or medium-sized environments, it's common for these administrative permissions to be held by the same (small) groups of people. Each step in the installation of Exchange requires a slightly different set of permissions for a company to be able to separate the administrative roles, should they desire to do so. If you have a single domain in your forest, to cover all the permissions, you should just assign a single account to Schema Admins, Enterprise Admins, and Domain Admins. If you use the GUI setup to skip all of the individual steps that follow, you'll need to have a user with all of those permissions.

The first step of the installation is to prepare AD with the permissions that Exchange will require. To execute this step requires that the user have Enterprise Admin and Domain Admin privileges in

the domain where the command is executed. In the D:\Exchange2010 directory, execute the command

```
setup.com
/PrepareLegacyExchangePermissions
```

This will execute fairly quickly. The next step is for Exchange setup to make required changes to the AD schema. These changes require Enterprise Admin and Schema Admin privileges for the user executing the command. Execute

```
setup.com /PrepareSchema
```

This command will take quite a while to execute.

The final preparation steps involve creating the required domain local groups for Exchange and setting up a variety of AD objects. The user executing the command must be a member of Enterprise Admins. Execute

```
setup.com /PrepareAD
```

If you have more than one AD domain, an Enterprise Admin should now execute

```
setup.com /PrepareAllDomains
```

Step 5: Installing Exchange Server 2010

To continue with the installation of Exchange, the user executing the installation must be a member of the (local) Administrators group on the Exchange-server-to-be and a member of the Organization Management group (which was created during the PrepareAD step above; the user who executed that step is already a member of the group).

At this point, continuing with the command-line neither simplifies nor complicates life. To install the various server roles using the command-line, use the command

```
Setup.com /mode:install /roles:ca,ht,mb
```

If you're using a PowerShell session, you'll need to quote the entirety of the /roles parameter.

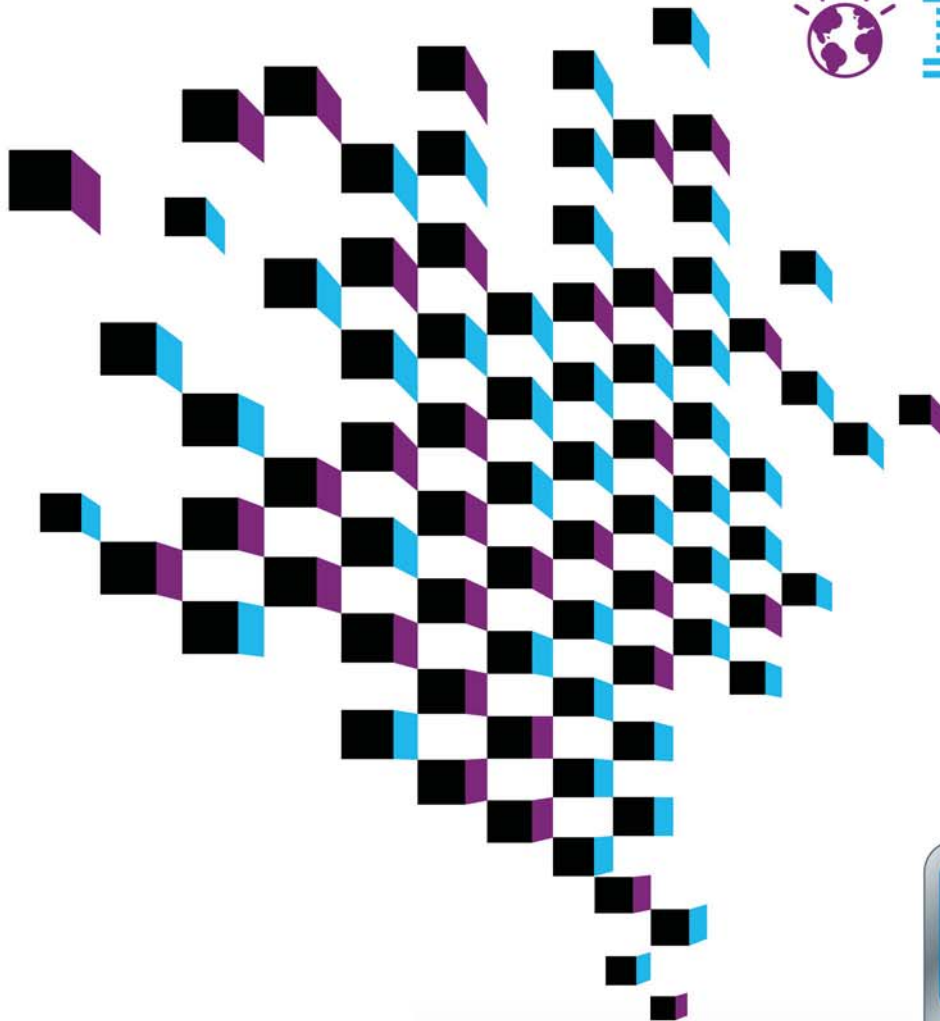
To use the GUI, double-click the Setup application in D:\Exchange2010. Click

Smarter technology for a Smarter Planet:

Thinking outside the box depends on what's in the box.

The systemic inefficiencies in many server rooms today, in terms of both energy consumption and utilization, are becoming unsustainable. A recent study found that an estimated half of all businesses experience IT outages due to power and cooling issues¹. Smarter tools like the IBM BladeCenter® HS22 can help. It's designed to give you greater efficiency at every level, from its highly efficient design and Intel® Xeon® Processor 5500 Series to its advanced management software like IBM Systems Director that actively monitors and limits power consumption. All of which can add up to 93% in energy savings over the previous generation of rack servers. Learn how you can see a return on your investment in as little as three months² at ibm.com/hs22

Systems, software and services for a smarter planet.



¹Source: IDC Market Analysis #215870, Volume 1, December 2008, Worldwide Server Energy Expense 2008–2012 Forecast. ²Return on investment and power savings calculation based on 11:1 consolidation ratio scenario of 166 Intel 1U 2 socket servers to 14 BladeCenter HS22 servers and savings in energy costs, software license fees and other operating costs. Actual costs and savings will vary depending on individual customer configurations and environment. For more information, visit www.ibm.com/smarterplanet/claims. IBM, the IBM logo, ibm.com, BladeCenter, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. Intel, the Intel logo, Xeon and Xeon Inside are trademarks or registered trademarks of Intel Corporation in the United States and other countries. © International Business Machines Corporation 2009. All rights reserved.

Exchange on a Domain Controller

Although Microsoft doesn't recommend installing Exchange on a domain controller (DC), primarily due to some security issues and the potential for memory exhaustion, it's a fully supported thing to do. Both Small Business Server and Essential Business Server from Microsoft install Exchange on a DC. For more information on this topic, see my blog at bit.ly/bkJXWx and the links it suggests.

Note, however, that Exchange must be installed after the server is promoted to being a DC and a group catalog server. Also, it's not supported to change that status for the server for the entire time that Exchange is installed on that server.

Step 3: Choose Exchange language option. You can choose to *Install all languages from the language bundle*, which will require you to download the language bundles over the Internet, or you can *Install only languages from the DVD*, which will install the 11 languages that Exchange 2010 supports for server installations. (The language pack bundle adds translations for client OSs). Select to install only the languages from the DVD. Now Step 3 will gray out, and you can select Step 4: Install Microsoft Exchange.

The first screen of the wizard is simply boilerplate. Click Next. The next screen requires you to say that you accept Microsoft's license terms to continue. If you accept those terms (which you must in order to continue), click *I accept* then Next. The next screen invites you to join the Error Reporting program. Make your decision and click Next.

The next screen finally asks something of substance. For this installation, I'll be doing a typical installation, so click Typical Exchange Server Installation. If required, select an alternate path for the Exchange program files.

The next screen is designed to save you lots of configuration, and I recommend you use it. Here, you'll specify what the external name of the Exchange server will be for Outlook Web App (OWA), Exchange ActiveSync, and Outlook Anywhere (which was known as RPC/HTTP in Exchange 2003). Enter the value and click Next.

When specifying this during installation of a Client Access server, there should be no need to configure the Offline Address Book (OAB) virtual directory or Exchange Web Services virtual directory. However, you can review most settings for these virtual

directories (and the other virtual directories, such as Exchange Control Panel) from within Server Configuration, Client Access. However, there are some capabilities that can only be configured from Exchange Management Shell (EMS) by using various PowerShell cmdlets, such as Set-WebServicesVirtualDirectory or Set-OABVirtualDirectory. I won't cover them here, but be aware that the capability exists.

The next screen of the wizard requires you to select a particular Exchange 2003 server that will be connecting to the Exchange 2010 Hub Transport server. Based on my scenario, you probably have only a single choice. Click Browse, select the proper Exchange 2003 server, and click OK to return to the wizard. Click Next. The next screen, similar to the Error Reporting screen, asks whether you want to join the Customer Experience Improvement Program. Your choice has no real effect on the installation.

On the next screen, the setup process evaluates whether the server meets all the prerequisites for installing Exchange 2010. If all the readiness checks pass, you're finally ready to install Exchange. Click Install.

Even on a fast server, installing Exchange takes quite some time—you can expect it to take at least 20 minutes, and on slower hardware it could take as much as an hour. When it's done, click Finish to continue. Close the Setup GUI application and move to Exchange Management Console (EMC).

Step 6: Configuring Exchange Server 2010

EMC will take a while to initialize, especially the first time you use it. Once the primary initialization is complete, expand Microsoft

Exchange On-Premises and click Server Configuration. Because you've just installed the first Exchange 2010 server in your organization, there should only be a single server. In the Actions pane (the rightmost pane), click New Exchange Certificate. In the first page of the wizard, enter a friendly name for the certificate, such as All-purpose Exchange certificate.

The next screen asks whether you're going to use a wildcard certificate with Exchange. You could do so, but it would require special configuration later. It can also cause security problems. (For information about potential security problems with wildcard certificates, see the article at bit.ly/9nO6Nn.) I won't cover using a wildcard certificate here.

In the Exchange Configuration screen, select and configure all the required services you want your Exchange 2010 server to provide. Your choices will include Client Access server configuration, including Outlook Web App on the Internet, Exchange ActiveSync, Exchange Web Services, Outlook Anywhere, Auto-discover, and a legacy domain name that will be used on the Exchange 2003 server when both servers are online at the same time. The names that will be placed on the SSL certificate request in this example will be `mail.clarksupport.com`, `autodiscover.clarksupport.com`, `legacy.clarksupport.com`, and `clarksupport.com`.

I won't cover using Federated Sharing services, Unified Messaging services, or assigning a certificate to POP3 and or IMAP. However, if you choose to use any of the above domain names for POP3 or IMAP, it's a simple matter of checking the box for those services.

The next screen shows the above list of domain names. You have the option of adding or subtracting any additional domain names that you want to be included in the certificate request and selecting the domain name that will be the first domain name on the certificate—this is called the *common name*. Note that the wizard automatically chooses the base domain name as the common name (in this example, `clarksupport.com`)—that's sufficient for most purposes. You should note the common name for future use.

The final screen requiring input is for specifying the organization and location of

Out with the old. In with the affordable.

Did you know? By replacing your aging servers with IBM® System x3650 M2 Express® servers powered by the Intel® Xeon® processor 5500 series, you could dramatically lower your IT operating expenses.

Here's how: 1. With more computing power, you can run your applications on fewer servers. 2. Running fewer servers means reducing software licensing fees. 3. Enhanced systems management helps lower operational costs. 4. New energy-efficient servers reduce power consumption and cooling costs. Doing more with less has never been so important. And thanks to the people and Business Partners of IBM, it's never been easier. Learn how IBM System x® could help you see a return on investment in as little as three months¹ at ibm.com/systems/3monthroi



IBM System x3650 M2 Express

\$3,439

or \$87/month for 36 months²

PN: 794764U

Featuring up to 2 Intel® Xeon® x5540 processors (2.53 GHz)
16 DIMM sockets 1333 MHz DDR-3 RDIMMs (128 GB max)

IBM System x3250 M3 Express

\$1,535

or \$39/month for 36 months²

PN: 4252E1U

Featuring Intel® Xeon® x3450 processor (2.67 GHz), 2x2 GB Open Bay with MultiBurner
DDR-3 ECC memory, up to 1333 MHz; 1 GB, 2 GB and 4 GB UDIMMs, 16 GB
UDIMM max;³ 1 GB, 2 GB, 4 GB and 8 GB RDIMMs; 32 GB RDIMM max³



IBM System Storage™ DS3400 Express

\$9,295

or \$235/month for 36 months²

PN: 172642X

External disk storage with 4 Gbps Fibre Channel interface technology
Scalable to 3.6 TB of storage capacity with 300 GB hot-swappable SAS HDDs
or up to 9 TB of storage capacity with 750 GB hot-swappable SATA HDDs



Try the IBM Systems Consolidation Evaluation Tool today

Learn how IBM System x could help you see a return on investment in as little as three months:

ibm.com/systems/3monthroi

1 866-872-3902 (mention 6N8AH26A)



¹To learn how the return on investment was calculated, visit ibm.com/systems/xroi. ²IBM Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on an FMV lease of 36 monthly payments. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice. ³Maximum UDIMM support for 16 GB when 4 GB DIMMs are available 1Q 2010, and maximum RDIMM support for 32 GB when 8 GB DIMMs are available 1Q 2010. IBM hardware products are manufactured from new parts or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, visit http://www.ibm.com/servers/support/machine_warranties. IBM makes no representation or warranty regarding third-party products or services. IBM, the IBM logo, System Storage and System x are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. All other products may be trademarks or registered trademarks of their respective companies. All prices and savings estimates are subject to change without notice, may vary according to configuration, are based upon IBM's estimated retail selling prices as of 10/2/09 and may not include storage, hard drive, operating system or other features. Reseller prices and savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. IBM may not offer the products, features, or services discussed in this document in other countries. Contact your IBM representative or IBM Business Partner for the most current pricing in your geographic area. © 2009 IBM Corporation. All rights reserved.

■ EXCHANGE 2010 MIGRATION

the company requesting the certificate. The information on this screen should match closely the information your domain registrar has on file for your domain. Figure 1 shows an example dialog box filled out.

The next screen allows you to confirm your choices. If you need to change or correct any information, do so now. When you're satisfied with the information displayed here, click New.

Presuming there are no errors, the certificate request is created and stored on your server in the location you indicated. Now you should submit the certificate request to the provider of your choice (such as DigiCert, GoDaddy, or many others). Once you've received the returned certificate, it's time to install the certificate on the Exchange server.

In EMC, click Server Configuration. Then, in the Results pane, click the friendly name you gave to the certificate request. Click Complete Pending Request in the Actions pane. In the wizard that opens, select the resulting file from your certificate provider (it should end in either a CER or CRT suffix) then click Complete. The certificate should be imported. Click Finish to close the wizard.

Again within EMC, click Server Configuration and then click the friendly name of the certificate in the Results pane. In the Actions pane, click Assign Services to Certificate. The new server will be selected in the first page of the wizard. The next page is titled Assign Services to Certificate—check the box for Internet Information Services. On the next screen, confirm your choice by clicking Assign, then click Finish.

Now it's time to enable Outlook Anywhere. In EMC, expand Microsoft Exchange On-Premises, expand Server Configuration, then select Client Access. In the Results pane, select the server you've just installed, then click Enable Outlook Anywhere in the Actions pane.

In the wizard, enter the external domain name you'll be using for Outlook Anywhere. I used mail.clarksupport.com in this example. The selection of Basic Authentication versus NTLM Authentication controls the security used for client access. Because you'll be using SSL with Outlook Anywhere, the default of Basic Authentication will work fine. Click Enable, then review the results of the wizard and click Finish.

If the common name of the new SSL certificate is different from the external domain name you'll be using for Outlook Anywhere, you need to further configure an Outlook Provider. Open EMS, and enter the command

```
Set-OutlookProvider EXPR  
-CertPrincipalName  
msstd:<certificate-common-name>
```

Now you need to modify the Default Offline Address List. You'll change the server responsible for creating and maintaining it from your legacy server to the new Exchange 2010 server. In EMC, expand Microsoft Exchange On-Premises, then Organization Configuration. Click Mailbox underneath Organization Configuration and select the Offline Address Book tab. There's usually only a single entry in the Results pane—Default Offline Address List—select it. Then click Move in the Actions pane. In the Move Offline Address Book dialog box that opens, click Browse. In the resulting dialog box, click the new Exchange server and then OK. Click Move and the move will be executed. Click Finish.

Next, it's time to create a Send connector so that the new server can send email to the Internet (which isn't possible by default).

For this discussion, the Send connector will either send email to the Internet or forward email to a third party for message hygiene and final delivery (this is typically called a gateway or edge email server). Within EMC, expand Organizational Configuration and click Hub Transport. Click the Send Connectors tab, then click New Send Connector in the Actions pane to start the New Send Connector wizard. On the first screen, enter a name for the Send connector, such as *Outgoing Email*, and select Internet as the intended use of the Send connector. Click Next.

The next screen is for configuring the address space handled by this Send connector. That is, you specify the set of Internet domains to which the connector will send. Because you'll have only a single connector, configure it to handle all Internet domains. Click Add and, in the SMTP Address Space dialog box, enter an asterisk (*) for the Address field and leave the Cost field at the default of 1.

Back in the wizard, the new address space is visible. The next screen, Network settings, allows you to configure how the Send connector will deliver email. If your Exchange server is going to deliver email directly to destination servers, leave everything on this window at the default of *Use domain name system (DNS)*. If you need

The screenshot shows the 'New Exchange Certificate' wizard, specifically the 'Organization and Location' page. On the left is a navigation pane with the following items: Introduction (selected), Domain Scope, Exchange Configuration, Certificate Domains, Organization and Location, Certificate Configuration, and Completion. The main area contains the following fields and instructions:

- Organization and Location**
Use this page to enter the name of your organization, organizational unit, location, and certificate request file path.
- Organization:** Clark Systems Support
- Organization unit:** HQ
- Location:**
- Country/region:** United States (dropdown menu)
- City/locality:** Rockville
- State/province:** Maryland
- Certificate Request File Path:** C:\Exchange-certificate-request.req (with a 'Browse...' button)
- Below the file path, it says: 'Specify the name of the request file in the text box below. Use the Browse button to select the folder where you want the request file to be created. The name must end with the extension ".req".'
- At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

Figure 1: Completing the Organization and Location page

email to be routed through another computer for final delivery, click the button for *Route mail through the following smart hosts*, then click Add. On the *Add smart host* dialog box that opens, enter the proper IP address or Fully Qualified Domain Name for the smart host, then click OK. You can enter as many smart host entries as you need. When you've completed any changes on this page, click Next.

The next screen, Source Server, should have the name of the new Exchange 2010 server and no other entries. Don't make any changes; just click Next. The New Connector page summarizes the configuration choices you've made throughout the wizard. Review the display, and if any of the settings need changing, click Back and make them. When you're satisfied with the results, click New, then Finish to close the wizard.

Next you must ensure that your new server can receive email from the Internet. By default, an Exchange 2010 server is installed with two Receive connectors, but neither of them can receive anonymous email—which is most email from the Internet. Therefore, you'll change the security on one of those Receive connectors.

Receive connectors are configured on a per-server basis. In EMC, expand Server Configuration and click Hub Transport. In the Results pane, click the Exchange 2010 server. Click the Receive connector with a name that begins with Default, then click Properties. Click the Permission Groups tab, select *Anonymous users*, then click OK.

Now you'll make sure that all public folder information from the Exchange 2003 server is replicated to the Exchange 2010 server. This happens in two pieces, with the first piece easiest to do from EMS. Open an EMS session and enter

```
cd $exscripts
.\AddReplicaToPFRrecursive.ps1
-TopPublicFolder \
-ServerToAdd $env:computername
```

The second piece is easiest to do from an EMC Toolbox application. In EMC, click Toolbox then double-click Public Folder Management Console. Expand System Public Folders. You can ignore the folders with names that start with OWAScratchPad and StoreEvents. For

EFORMS REGISTRY, OFFLINE ADDRESS BOOK, and SCHEDULE+ FREE BUSY, you must ensure that each of their subfolders has a replica on the new server. (The EFORMS REGISTRY folder may have zero, one, or two subfolders.)

You're interested in changing the replicas for the subfolders that exist only on the Exchange 2003 server. As an example of checking which subfolders are only on the Exchange 2003 server, click SCHEDULE+ FREE BUSY, as shown in Figure 2. The subfolder with a name that begins EX:/o=Clark/ou=Exchange Administrative is selected in the Results pane. Click Properties in the Actions pane, then click the Replication tab. Note that the only server mentioned for this subfolder is the new server. Therefore, you won't need to add a replica for this subfolder. Click Cancel.

Now select the second subfolder, which is named EX:/o=Clark/ou=HQ in this example. Click Properties in the Actions pane, then select the Replication tab. In this case, the only server listed is the legacy Exchange 2003 server, so the Exchange 2010 server needs to be added. Click Add. In the Select Public Folder Database dialog box, click the name of the new Exchange 2010 server and then OK. Now the Replication tab will contain both the old and the new server and should have a replication list that includes both the legacy Exchange 2003 server and the new Exchange 2010 server. Click OK to close the dialog box.

To complete updating public folders, repeat this process with each subfolder in the OFFLINE ADDRESS BOOK folder and the EFORMS REGISTRY folder. When you've updated them all, close the Public Folder Management Console. Next, configure the Exchange 2003 OWA URL that Exchange 2010 will use to refer OWA clients whose mailboxes are hosted on the Exchange 2003 server. For this example, open an EMS session and enter

```
Set-OWAVirtualDirectory Clark2008\OWA* `
-Exchange2003URL "https://legacy
.clarksupport.com"
```

A common request is that when a user accesses the root of an Exchange server, the user be automatically redirected to OWA. This is easily done by placing the lines below into a file on the Client Access server named C:\inetpub\wwwroot\Default.htm:

```
<html>
<head>
<meta http-equiv="refresh"
content="0;url=https://mail
.clarksupport.com/owa">
</head>
</html>
```

You'll need to update the name of the website (mail.clarksupport.com) to match the external name that you specified when you installed the CAS. If you wonder why I didn't use Default.asp and have this URL automatically generated, it's because

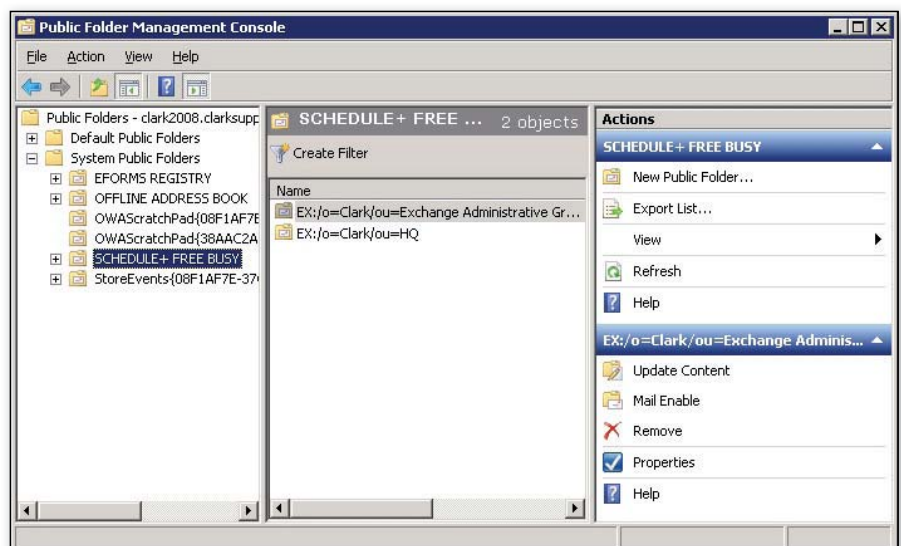


Figure 2: Locating subfolders of SCHEDULE+ FREE BUSY

■ EXCHANGE 2010 MIGRATION

the ASP module isn't installed into IIS by Exchange-Typical.xml because Exchange itself does not require it.

Step 7: Configuring Exchange Server 2003

Forms-based authentication must be set on the Exchange 2003 server for OWA to allow for seamless transfers from the Exchange 2010 server. Using the MMC Certificate Manager snap-in or EMC, you should now export the SSL certificate that you created earlier to a PFX file (making sure to export the private key). Copy the .pfx file to the Exchange 2003 server and import the key there, also using the Certificate Manager snap-in.

Using the IIS Management Console, modify the properties of the Default Web Site to use the new SSL key. This lets the old Exchange server accept both the legacy name (legacy.clarksupport.com in this example) and the current name (mail.clarksupport.com) until DNS is updated. After the update, execute iisreset or reboot the old server to begin using the new certificate.

Once you've made this certificate change, Outlook configurations using RPC/HTTP on the Exchange 2003 server will no longer work. You have two options: create a new Outlook MAPI profile using the new parameters, or modify the existing profile for those users. To make the modification requires you to be aware of the legacy name that will be used for the old Exchange 2003 server and the common name of the SSL certificate that was created and loaded (clarksupport.com in this example).

How you access the Connection properties of Outlook varies between versions. In Outlook 2007 and later, you can click on the account properties, then More Settings, then the Connection tab. If the Connect to Microsoft Exchange Using HTTP box isn't selected, this profile isn't using RPC/HTTP. If it is selected, click the Exchange Proxy Settings button. Prior to correction, for this example, the dialog box looks like Figure 3. To continue to allow RPC/HTTP to work for mailboxes hosted on the old server, you'll need to make the changes shown in Figure 4.

You have to make these changes only if you're using Outlook 2003 or if the mailbox is going to stay on the old server for some time. If you're using Outlook 2007 or later and you've configured Autodiscover, when you move the mailbox to the new server, the Outlook profile will be automatically reconfigured. If you have more than one Exchange 2003 server, you'll need to suppress link state updates, as described in a TechNet article at bit.ly/aICc3q.

Configuring DNS

At this point, you're ready for the rubber to meet the road. It's time to update your internal and external DNS so that the legacy name properly points to the Exchange 2003 server (legacy.clarksupport.com) and the external name you used to configure the Client Access server points to the new Exchange 2010 server (mail.clarksupport.com).

For Outlook redirects and Autodiscover to work properly, the external

name for the Client Access server on your internal LAN must resolve internally to an IP address that can be accessed internally. The same is true for the legacy Exchange server name. Make the DNS updates and test. If you've followed all the steps, both servers should seamlessly work together.

Your next step is to migrate your mailboxes, a subject that's covered in detail in the article "Moving Mailboxes the Exchange 2010 Way," InstantDoc ID 103651.

A Job Well Done

You should now be up and operating in a coexistence environment. Once all your mailboxes are moved, you can begin the process of decommissioning the Exchange 2003 environment. However, don't just cut off that server! Although you're now operating in a coexistence environment, there are a number of items, such as OABs and email address policies, that must be transferred from the old Exchange environment to the new one. Please consider referring to my blog for further information. And enjoy using Exchange 2010 and the many enhancements it offers.

InstantDoc ID 104657

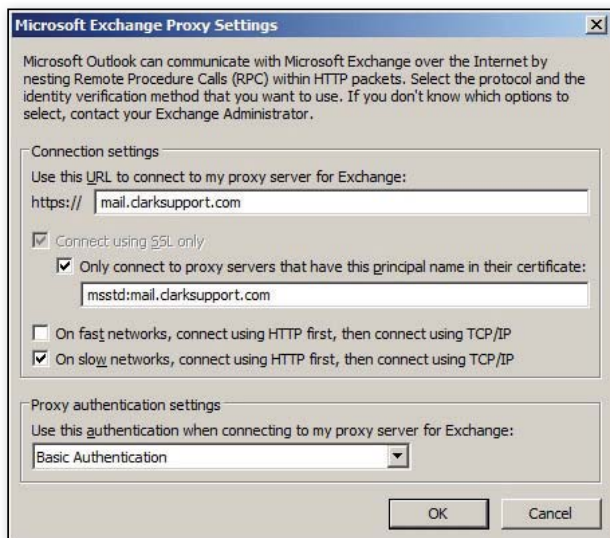


Figure 3: Exchange proxy settings prior to correction for old server

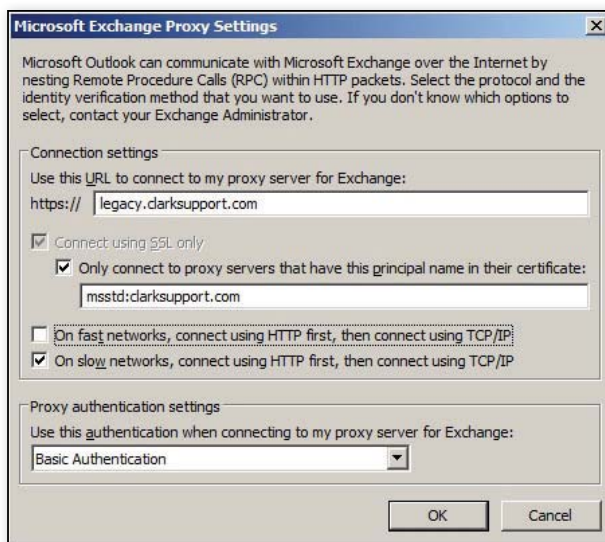


Figure 4: Exchange proxy settings after correction for old server



Michael B. Smith

(Michael@theessentialexchange.com) is an independent consultant and a Microsoft Exchange MVP. He's been using Exchange since version 5.0 and working with messaging applications since 1981. He has a blog at theessentialexchange.com.



Microsoft Helps Smooth Your Exchange 2010 Transition

It's been roughly six months since Microsoft Exchange Server 2010 was released into the wild of the business world—time enough, certainly, for IT departments to get familiar with the new mail server and what it has to offer and determine whether to push their organizations toward an upgrade. Naturally, Microsoft hopes you'll move to the latest version, and the company has taken great steps to help you make the transition as easy as possible. I recently spoke with Rajesh Jha, corporate vice president for Microsoft Exchange, about what Microsoft is doing to prepare companies and about some of the tricky points of Exchange 2010's new features that IT pros should be prepared for.

(Editor's Note: For the full interview, including Jha's views on competition in the cloud, see the online version at www.windowsitpro.com, InstantDoc ID 104656.)

B. K. Winstead: Let's start by looking at what Microsoft is doing to help customers make the transition. For instance, you have the Exchange Server Deployment Assistant on your website (technet.microsoft.com/exdeploy2010/default.aspx), which was recently upgraded to include additional deployment scenarios that weren't available when Exchange 2010 launched. Are you planning to continue adding other scenarios, such as migrating to cloud-based Exchange or using virtualization?

Rajesh Jha: We've gotten very positive feedback on the Deployment Assistant from our customers. What the wizard does is, instead of having customers go and find all the relevant stuff that applies to their configuration, it gives them a higher-level wizard to navigate their specific circumstances and find the white papers or documentation that's relevant for their situation.

But at the same time, we don't have all the flavors in the deployment wizard today. The documentation exists for all of these [scenarios], so we will continue to add more steps in the wizard as we get more feedback. As people say, "Hey, I wish virtualization was called out," then we will add that. We'll add online. We think this is a very scalable way for us to guide our customers. It's scalable in a personalized way. It's absolutely something we'll continue to invest in.

The Exchange node on TechNet [technet.microsoft.com/en-us/exchange/default.aspx] [has] a whole section on how best to migrate to Exchange 2010. The wizard is just a higher-level overlay on the set of content that we have there. The other thing we've done this time is—Exchange used to always provide guidance in the Storage Calculator—we've enhanced that significantly. [It's now called the Exchange 2010 Mailbox Server Role Requirements Calculator and is available at msexchange.com/files/12/attachments/entry453145.aspx.] Again, this is very customizable—depending upon the storage type, how many copies they want to use, the kind of disaster-recovery capabilities they want to build in. We provide guidance to customers in terms of how to size their disks, how to size their CPUs, and memory usage. So we've built not only the deployment wizard, which is more like a step-by-step process, but also sizing guidance that is personalizable for the different configurations that our customers might need.

**Exchange VP
Rajesh Jha talks
about migration
tools, architectural
changes, and how
implementing
Exchange 2010
will save you
money**

by B. K. Winstead



Rajesh Jha, corporate vice president for Microsoft Exchange

Winstead: One of Microsoft's key talking points at the time Exchange 2010 was released was that it would save organizations money. Is that message sticking with people? Or are budgets still too tight for companies to make such a major switch?

Jha: I think the Exchange 2010 story of cost savings is very strong, and it's still resonating with customers. Not all the saving mechanisms apply to all customers, but there is so much in it that something applies to almost any customer. There are customers that have been able to increase their storage size significantly and provide much bigger mailboxes to their end users while reducing their costs byte by byte based on what they had on Exchange 2003 by just moving to cheaper storage options in Exchange 2010. There are customers that have been able to get rid of their parallel investment in backup or disaster recovery because in Exchange 2010 we have the database availability group where customers get to choose how many copies of the data that they have. We've unified the notion of backup and availability and disaster recovery into one architecture.

Then there are customers that had a parallel system for voicemail, and with Exchange 2010 we allow, on the same Exchange servers, for you to be able to offer unified messaging and voicemail. That's another cost-savings option. Around 80 percent of customers don't have archiving today, but the vast majority of them see some need to get archiving into place. Again, with Exchange 2010 the same email infrastructure allows you to do archiving, retention, discovery. And finally, for our smallest customers, the promise of either being on-premises or in the cloud, that's another cost savings. They can just move to the cloud and they'll get the exact same functionality of Exchange 2010 in the cloud as they do on-premises. If you take a look at the body of case studies we have on Exchange 2010, it's incredible just the wide variety of cost savings our customers have been able to realize.

Winstead: You mentioned the ability to use database availability groups (DAGs) to eliminate third-party backup solutions. I suspect there will be some organizations that will resist this idea or be afraid to give up their backups. Do you see a particular size or

type of organization that will be most willing to rely on DAGs for backups?

Jha: You raise a really interesting observation, which is the notions of high availability, backup, archiving, compliance—some customers will combine these concepts in one implementation. So there are some customers for whom their backup is also their archive is also their compliance, or the store they would go to for retention, and so on. But for many customers, they do tend to be discrete concepts and discrete workflows. And so the database availability group doesn't mandate that you have to think about all four of these concepts implemented on top of the database availability group. But you could use this for all four of these.

So who would take advantage of the backup capabilities that have been built into the database availability group? We've actually seen customers of all sizes. Here at Microsoft, we run our backup exclusively on database availability groups. The 200,000 mailboxes at Microsoft are actually implemented on that mechanism. The service that we're running for 20 million educational customers runs on that infrastructure. We have smaller customers—there are case studies, I forget the exact number of seats but it's not a lot—that have actually gone with this mechanism for their backup needs. But there will be customers that will say, "No, I'll use database availability groups for high availability and disaster recovery, but I want to stick to my existing backup process." And that's fine, too.

Winstead: You mentioned the archiving feature in Exchange 2010—that's something that you're offering for the first time with this release. I know people I've spoken with have real concerns that the archive is stored on the same server as the primary database, which isn't the traditional way you think about an archive. At this point, do you have any idea of how you'll be developing the archiving feature either in service packs or future releases of Exchange?

Jha: Let me start by talking about what the archive feature in Exchange 2010 is. It allows the IT pro to solve the PST problem. Most organizations today have a bunch of PSTs that aren't under management by the IT pro. And it's not that the end user has a

great experience. I mean, if you have a PST on your primary desktop, you can't get to it or do a search on it when you're on your mobile device or on a browser or a different desktop. So by bringing all these PSTs in, a couple of things happen. The IT pro is now able to manage these, and do discovery against these. And the end user gets anywhere access, so now you can do a search across your PSTs—what used to be your PST is now your online archive, and it's available to you from anywhere.

And we have capabilities for the IT pro to put legal holds, do discovery, without having a separate infrastructure for archiving. Many of our customers need that. Customers that don't have archiving today are able to get that on their messaging infrastructure. We've received feedback that's saying they aren't comfortable with the archive and the primary mailbox being in the same database. And it's feedback we've heard loud and clear, and we're working through our plans on how best to address it. I don't have anything to share at this time, but yes, we do have the feedback.

The one thing I would offer up, though, is it's not something that actually increases their costs, the way it's implemented today. If anything, I think it offers an opportunity to reduce costs. If you think about the costs of storage, what you end up paying for is the speed of the disks. You don't end up paying that much for the size of the disk. The disks are getting bigger and bigger and cheaper and cheaper. What's not getting cheaper is how fast these disks go. If you think about how storage and archives are accessed by the end user, it's sporadic access. It's not something you go back to. The half-life of email isn't very long.

So if you co-locate email that's accessed very, very rapidly with lots of storage that isn't accessed very often—in other words, you co-locate hot storage and cold storage—then you're taking advantage of the laws of physics, where the disks are getting bigger. The disks aren't getting faster, but you don't need more speed for the archive to be co-located because it's not accessed that often. If you keep the archive and the primary mailbox in two different databases, you're going to end up paying for the spindles separately anyway.

For some set of customers, the opportunity to co-locate hot storage and cold

storage is exciting because it offers them over the long run substantially reduced storage costs.

Winstead: For people currently on a different mail platform altogether, what should they think about when considering a move to Exchange 2010?

Jha: They should definitely take a look at our cloud option with Exchange Online. Most of our customers today actually have been folks that have moved from either Lotus Notes or Novell GroupWise. It's a very exciting option to many customers because now they don't have to build a lot of expertise running Exchange on-prem—they can let Microsoft do that and keep their service ever-green with the latest version of Exchange available to them. Whether they run Exchange today or they don't, that's one of the decisions they should walk through: Where do they fall between wanting more control versus delegating more to Microsoft to run in the cloud?

There will be customers that will choose to be kind of in the middle—they may move a set of users to the cloud and keep a set of users on-premises. They'll have free/busy inter-op between the two, between the cloud and on-premises. They will be able to move mailboxes back and forth, the same manageability tools, the same end-user features. So I think that's a very important consideration in the design of their infrastructure: Cloud or not? If cloud, is it everybody in the cloud or is it some set of folks in the cloud?

Winstead: Some people I've spoken to in the industry seemed to reject the hybrid option, thinking it would be too complicated to implement and manage.

Jha: I really think it depends upon the specific organization. For some organizations, it may not be worth having a hybrid. They may want to say, you know, we want to have one Help desk control flow to deal with, whether it's on-premises or fully in the cloud. And that's OK. That's what I feel is the Exchange 2010 choice of flexibility for our customers.

But I do think there will be some large customers for whom hybrid will be the way it's going to be. Even if they decide

to move their entire messaging infrastructure in the cloud, they may choose to have their collaboration on-prem, or their directory will probably be on-prem. So some level of hybrid is true for most large organizations, whether it's in transition phase, whether it's a different workload, whether it's a directory. Some of them actually have structured workers or branch offices in the cloud but keep their corporate office on-prem. Our customers don't come in one size and we don't want to be prescriptive in how they should run. They know what their needs are best, and we want to support them in whichever configuration they want to run.

Winstead: And if you set up a hybrid configuration, is it still manageable through one management console?

Jha: Yes, that's the cool thing. If an IT pro decides, "I want to bring this person back in house," it's the same management console. It's an online move. You don't even have to recreate the Outlook offline cache—you just move the user, and they're ready to go.

Winstead: What are some of the big changes in Exchange 2010 for admins already familiar with Exchange 2007?

Jha: One of the biggest changes that we made is in the Client Access role in Exchange 2010. In the past, Outlook would go directly against the Mailbox role whereas Outlook Web App and mobile [connections] would go through the Client Access role. So one of the nice things we've done in Exchange 2010 is that we have Outlook, Outlook Web App, and the mobile access—all the client access—actually goes through the Client Access role now.

This does a couple of really interesting things. One is it allows us to provide a much more consistent experience across all of these devices or all of these different clients in terms of business logic. For instance, calendaring consists of lots of business rules; so what should happen with calendaring [on each of these different clients]? Now we've got that centralized all in one place. You get a consistent experience no matter what device you're on.

And the second thing is our high-availability story. This was enabled with

this architecture because the Outlook line now virtually binds to a mailbox and the Client Access role can abstract away which copy of the database you are actually binding to without having to restart Outlook. So, it has become a more important role than in Exchange 2007. If you take a look at our deployment wizard, it's heavily weighted toward walking our Exchange 2003 customers and Exchange 2007 customers over how to manage the rollout of Client Access in their organization—it's a step-by-step process.

Winstead: Microsoft has so many new releases out or coming out. IT departments will need to look carefully at what they need before jumping into any of these purchases. What will make Exchange 2010 stand out from this group?

Jha: Messaging is a key workflow. I think it's a recognition of how important communication and collaboration is to our customers in terms of the value that their businesses are able to drive. That's number one: The business value we're able to offer with Exchange 2010 is very strong.

At the same time, they actually get to save money. If you take a look at the Forrester study ["The Total Economic Impact of Microsoft Exchange 2010," download microsoft.com/download/7/5/0/75068B44-0A70-4BBF-9824-01ECF076F7AE/TheTotalEconomicImpact_pdf_11042009.pdf], it just reiterates what we've seen with all our case studies so far: Our customers will be able to save money by moving to Exchange 2010. You've got a mission-critical infrastructure. Your user needs continue to grow. You can add business value. And we are confident that we will save our IT pros money by making this change to 2010. And then the truth of the matter is a large installed base of Exchange customers today are on Exchange 2003. That product and their hardware is at end-of-life. Exchange 2010 is a great option for them. 

InstantDoc ID 104656



B. K. Winstead

(bwinstead@windowsitpro.com) is an associate editor for *Windows IT Pro*, *SQL Server Magazine*, and *System iNEWS* specializing in messaging, mobility, and unified communication.

Deploying Database Availability Groups in Exchange Server 2010

Achieve a strong, highly available design with this mailbox-resiliency foundation

by Paul Robichaux

Microsoft adds new features to every Exchange Server release. Some of these features are destined to be quietly ignored and eventually retired—remember the Exchange Network News Transfer Protocol (NNTP) server? Others go out in a quick blaze of glory, such as active/active clustering. Still others introduce fundamental changes in the way we design and deploy Exchange. Exchange 2010's new database availability group (DAG) feature falls into that last category. The idea of providing mailbox resiliency by distributing multiple copies of mailbox databases throughout the Exchange organization is solid, and its implementation in Exchange 2010 marks a major change for high-availability designs.

Tony Redmond's "Exchange 2010: High Availability with DAGs," InstantDoc ID 102925, describes the technical fundamentals behind DAGs. If you're not familiar with the basic underlying concepts, it's worth a read before tackling this article, in which I'll focus on how to deploy simple DAGs. But first, let's talk about prerequisites and other considerations.

DAG Prerequisites

The first, and biggest, prerequisite for DAG deployment is simple: You must be using Windows Server 2008 or 2008 R2 Enterprise Edition. If you have Standard Edition deployed, you won't be able to place DAGs on that server unless you reinstall Windows. There's no in-place upgrade from Standard to Enterprise. Unfortunately, that means that if you have a Standard Edition server that's already running Exchange, that server can't be a DAG member server until you upgrade it. This predicament has affected many sites that have experimented with early deployments of Exchange 2010 on Server 2008 Standard, intending to upgrade their mailbox servers to DAG membership later.

From a network standpoint, DAG prerequisites are fairly straightforward. Exchange 2010 uses slightly different terminology from that of Exchange 2007. The *MAPI network* on a DAG member is for communicating with other Exchange servers and Active Directory (AD), whereas the *replication network* is for database replication traffic. In a significant change from Exchange 2007, Exchange 2010 now supports the use of a single network interface for both MAPI and replication networks, although the preferred design is still to use separate NICs and networks for those two functions. If the MAPI network interface fails, the server will fail its databases over to another DAG member. However, if the replication interface fails, replication traffic will silently move over to the MAPI network, reverting to the replication network when it becomes available again.

You can specify multiple replication networks, which is useful for complex topologies. However, every member of a given DAG must have the same number of networks defined. All members of a

DAG should be able to communicate with no more than 250ms of network latency, but Microsoft warns that overall network performance is important, too—not just the latency measurements.

There are a couple more restrictions to keep in mind. All the members of a given DAG must be members of the same AD domain, although different DAGs can be members of different domains. And DAG names must be unique within the organization, and they must be 15 characters or fewer in length. (DAGs are the last remaining vestige of WINS remaining in Exchange. Perhaps the next version will get rid of it altogether.)

Can I Get a Witness?

Before we dive into building your first DAG, we need to talk about the role of the *witness server*. If you're familiar with clustering, you'll recognize the underlying concept of a quorum resource. The quorum is essentially a way for all the nodes in the cluster to know which nodes are in the cluster and which are active or failed at a given moment. Despite the fact that Microsoft avoids the word *cluster* when discussing DAGs, the fact remains that DAG members need a way to tell which DAG nodes are active and which aren't. The Active Manager keeps track of this status, but it needs a way to store that status information in DAGs that have an even number of members.

Enter the witness server, which is nothing more than a file share on any Windows server in the forest. Microsoft recommends that you put the witness on a Hub Transport server so that it remains under the control of an Exchange administrator. The witness for a DAG can't reside on any Mailbox server that's a member of the same DAG. (It's legal to put the witness for one DAG on a member of a different DAG, but from a resiliency standpoint, that isn't a great idea.) The server hosting the witness must be a member of the Exchange Trusted Subsystem

Before we dive into building your first DAG, we need to talk about the role of the witness server.

security group. The system adds Exchange 2010 servers to this group during installation, but if you're locating the witness on another type of server you'll need to verify that the server is added to that group.

When you create a DAG, you can optionally specify the server and directory to use for the witness. If you don't specify these parameters, Exchange will try to locate the witness on a Hub Transport server that doesn't also

have the Mailbox server role and will put the witness on the first one it finds.

When you create a DAG with an even number of nodes, Exchange automatically creates the witness share and related data on the server you specify. If you change a DAG with an even number of nodes by adding or removing a node so that it has an odd number of nodes, Exchange will helpfully remove the witness. You can see where this is going: If you grow your DAGs by adding individual nodes, prepare for a lot of excess flailing as Exchange adds and removes the witness each time the number of member servers changes.

Suppose you want to build a two-node DAG—the simplest possible configuration. The DAG itself will have a unique name and IP address, which might be static or DHCP-assigned. If you have multiple subnets in your MAPI network, you need one IP address in each subnet for the DAG. To keep things simple, we'll assume that our MAPI network has a single subnet, 172.16.250.x.

The initial step, now, is to install Windows Enterprise Edition on the DAG member servers. Once that's done, we can proceed to install Exchange 2010's Mailbox server role. At that point, the fun begins! There are several distinct steps to getting a DAG up and running. First, you create the DAG itself, then you add servers to it, then you allow seeding and replication to complete. Let's tackle these steps in order.

Creating a New DAG

You can create DAGs by using the `New-DatabaseAvailabilityGroup` cmdlet or the New Database Availability Group wizard in Exchange Management Console (EMC). Figure 1 shows the first page of the wizard with a DAG name, witness server name, and witness directory specified. Click the New button to create the DAG object in AD, and it will immediately appear in the Database Availability Groups tab of the Mailbox view of the Organization Configuration node in the EMC, as Figure 2 shows. This view shows you the DAGs that exist in your organization and which servers are in them. If you want to see which mailbox databases are in which DAGs, you'd use the Database Management tab, which lists all the known mailbox databases and shows which server (or servers) hosts each one.

The newly created DAG is just an AD container object; it doesn't yet have any

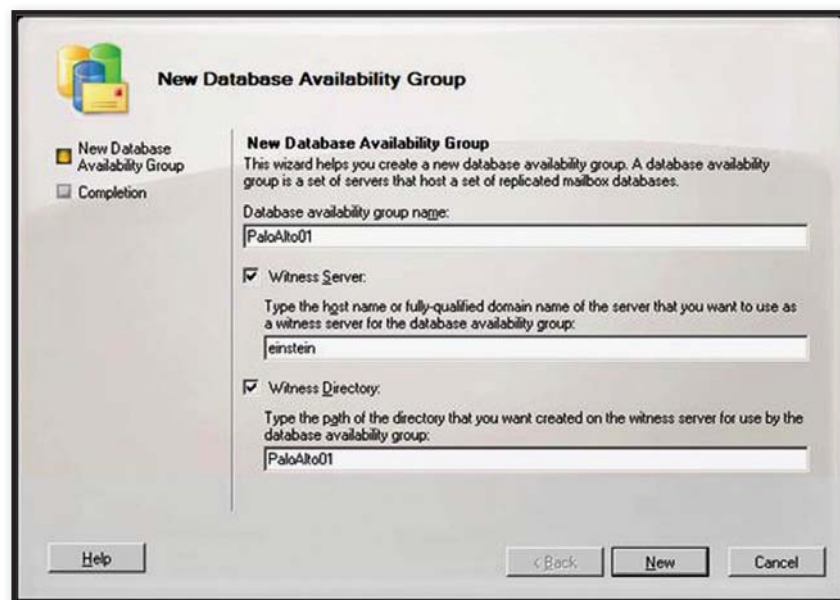


Figure 1: The New Database Availability Group wizard

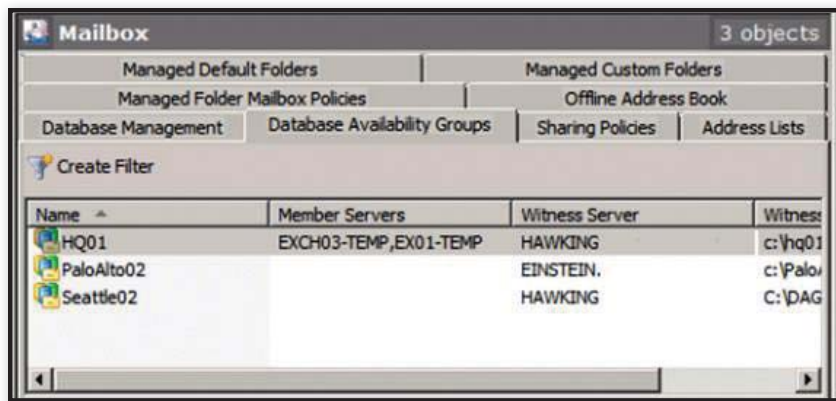


Figure 2: A view of multiple DAGs

servers or networks assigned to it. By default, your new DAG will get an IP address via DHCP. You can assign an IP address after the fact with the `Set-DatabaseAvailabilityGroup -DatabaseAvailabilityGroupIPAddresses` switch, which lets you set IP addresses *only for the MAPI network*. Don't use this to assign IP addresses for the replication network. It's usually easier to do this as part of creating the DAG from Exchange Management Shell, as follows:

```
New-DatabaseAvailabilityGroup -name
  Seattle01 -WitnessServer einstein
  -DatabaseAvailabilityGroupIPAddresses
  172.16.241.105
```

Managing DAG Membership

Of course, the new DAG can't do anything until you add servers to it. To do so, you can use the Manage Database Availability Group Membership wizard in EMC (right-click the DAG object to start it) or the `Add-DatabaseAvailabilityGroupMember` cmdlet. In either case, all you need to do is pick the Mailbox servers you want to add to the DAG, and Exchange does the rest of the work.

This explanation is deceptively simple because Exchange is actually doing an awful lot of work behind the scenes:

1. If it's not already installed, the Windows Failover Cluster (WFC) component of Windows Server is installed. This is roughly equivalent to setting up a Windows cluster, so it's nice to have this happen automatically.
2. The system creates a new Windows failover cluster object, using the name you specified for the DAG. Exchange uses only the cluster heartbeat, cluster database, and cluster network list.

3. The system registers a new A record with the name and IP address of the DAG in DNS.

4. The system adds the server as a member of the DAG object in AD.

5. The system updates the WFC database to include the new server and the databases that are mounted on it.

6. The Active Manager receives information about the new database copies on the newly added node.

When you add more nodes to the DAG, the same basic steps take place. One additional step is required, however: The WFC model might need to change between node majority (if the DAG now has an odd number of members) or node and witness majority (if the

After you create a DAG, you still have some things to do before it begins protecting your mailbox data.

DAG now has an even number of members). You can remove nodes from a DAG, but before you do so, you must remove the replicated mailbox database copies it contains. Use the `Remove-DatabaseAvailabilityGroupMember` cmdlet or EMC for that purpose.

Managing Mailbox Databases

After you create a DAG, you still have some things to do before it begins protecting your mailbox data. Namely, you have to

specify which mailbox databases should be replicated to it. To do so, you add mailbox database copies to the DAG with the `Add-MailboxDatabaseCopy` cmdlet or by right-clicking the database in EMC and using the `Add Mailbox Database Copy` command.

Adding a mailbox database copy to a DAG member server instructs that server to start maintaining a replicated copy of the database. This procedure takes place in two phases. First, the database copy must be seeded: Exchange copies data from an existing replica to the new replica. Once the system has streamed the full database to the new target, it copies each new log file generated over a TCP socket connection, then replays it into the replica copy.

The seeding process as outlined in the Microsoft article "Managing Mailbox Database Copies" (technet.microsoft.com/en-us/library/dd335158.aspx) contains 28 distinct steps. Here's a brief summary:

1. Exchange performs several pre-requisite checks to ensure that the source database and log files exist, and that the target location can receive the seeded data.
2. The Microsoft Exchange Replication service on the target requests that seeding start.
3. The Microsoft Exchange Replication service on the source suspends replication of the source database.
4. The target sends a request to start the actual flow of seeding data.
5. The source server opens a backup session using the familiar Extensible Storage Engine (ESE) streaming backup API.
6. The data collected from the source database is fed to the Microsoft Exchange Replication service, which feeds it over the replication network to the replication service on the target.
7. Once the complete database has been seeded, the newly created database copy moves to its final location.

The amount of time required for seeding will vary depending on the size of the database and the amount of bandwidth available on the replication network. It's impossible to give even a rough estimate of the time required without knowing these two factors.

Sometimes a database copy will diverge from the original master copy. This can happen as the result of a network interruption or a hardware failure, for example. When

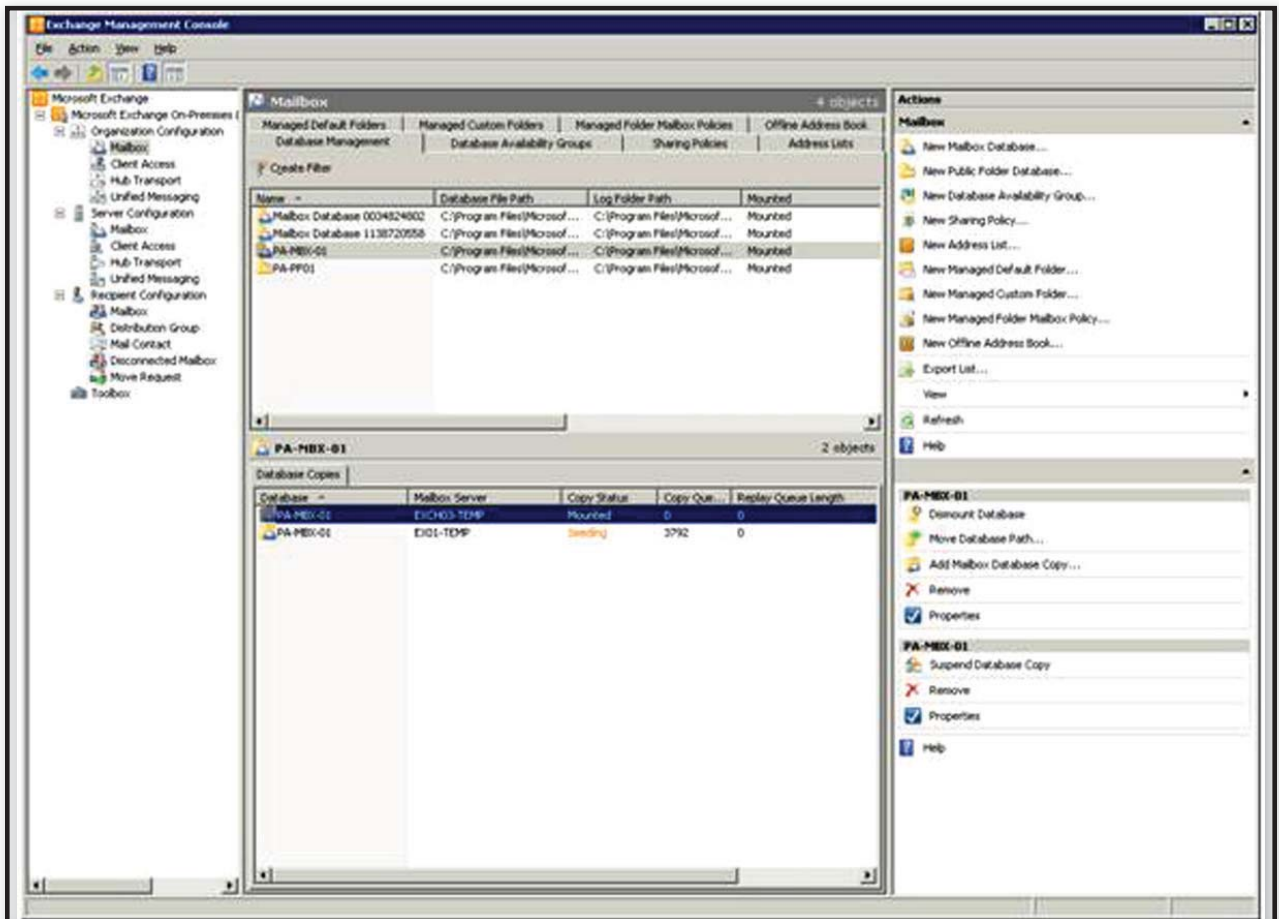


Figure 3: The Database Management view

a copy diverges, it needs to be reseeded. Exchange will automatically seed a database only when you create a new one; if you have a diverged database, you must manually reseed it. To do so, you can use either the `Update-MailboxDatabaseCopy` cmdlet or the Update Database Copy wizard in EMC.

Operating with the DAG

After you have the DAG set up and the database copies added, during normal operation you don't have to do anything other than monitor the health of your replicated databases. The Database Management tab in EMC, which Figure 3 shows, displays the status of each copy of the database: seeding, healthy, dismounted, and so on. The Active Manager will take care of activating the appropriate replica of the database if the active copy fails.

You can also manually activate an individual database copy with the `Move-ActiveMailboxDatabase` cmdlet (or from EMC). Manually activating a database copy is called a *switchover*; when Exchange does the

same thing automatically, it's called a *failover*. No matter what you call it, the Active Manager infrastructure takes care of notifying other Exchange components (e.g., the RPC client access layer) so that clients are able to connect to the newly activated mailbox copy.

Does It Work?

Does this technology work? Absolutely. I recently deployed Exchange 2010 at a company that had been using a Linux mail server. During the first week after the deployment, someone accidentally unplugged and relocated one of the physical hosts that ran the virtualized mailbox server. No one noticed! There was no impact to users, and the failover wasn't discovered until someone noticed that the physical server was no longer in its original location.

DAGs provide a very broad set of design options. RAID or Just a Bunch of Disks (JBOD)? How many DAG member servers? How many database copies? Should you colocate the Hub Transport, Mailbox, and Client Access server roles on two-node

DAGs? If so, how do you handle failover and load balancing for the Client Access role? One of the best things about the technology underlying the DAG feature set is that it can be adapted to a wide range of situations, including both site resiliency and mailbox high availability. As organizations get more experience designing, deploying, and operating Exchange 2010 with DAGs, I expect we'll see the emergence of a few basic "building block" designs that can be adapted to individual circumstances—and that in itself would be a major advance for Exchange high-availability design and deployment.

InstantDoc ID 103536



Paul Robichaux

(probichaux@windowsitpro.com) is a senior contributing editor for *Windows IT Pro*, a content author at Acuitus, and a Microsoft Exchange MVP and MCSE. Paul is the author of *Exchange Server Cookbook* (O'Reilly and Associates) and blogs at www.robichaux.net/blog.

PROBLEM:

You need to deploy an OS to a computer that isn't connected to your network.

SOLUTION:

Use MDT to create a bootable image for a DVD or external drive.

WHAT YOU NEED:

Microsoft Deployment Toolkit 2010, steps from "XP to Windows 7 Migration with Microsoft Deployment Toolkit 2010," InstantDoc ID 103607

SOLUTION STEPS:

1. Create selection profiles
2. Create your media
3. Update your media
4. Prepare your media
5. Use your media on the client machine
6. Customize or automate your media (optional)

DIFFICULTY:

Create Windows 7 Media for Deployment

No network, no problem—use MDT to create media and deploy from portable storage

by Rhonda Layfield

The Microsoft Deployment Toolkit 2010's media feature lets you deploy a complete OS, including applications, drivers, and packages from a DVD (size permitting), external hard drive, or universal flash device (UFD—a USB storage device with flash memory) without any network connectivity at all. You can mail the media to a branch office manager, who might also be the resident IT admin. All the office manager has to do is boot from the media, answer a few questions (which can be automated), and voilà—OS deployment completed in accordance with your corporate standards.

In this article, I'll show you how to create a Lite Touch bootable ISO image that contains the Microsoft Deployment Toolkit (MDT) components needed for an OS deployment. I'll begin by showing you how to create a selection profile; create, update, and prepare the media; and automate the client's deployment wizard.

This article assumes you've performed Steps 1-5 from April's article, "XP to Windows 7 Migration with Microsoft Deployment Toolkit 2010," InstantDoc ID 103607. If you've completed these steps, you should have the following:

- A deployment share created by accepting all defaults (F:\DeploymentShare)
- An imported Windows 7 x64 full set of source files (accepting default settings)



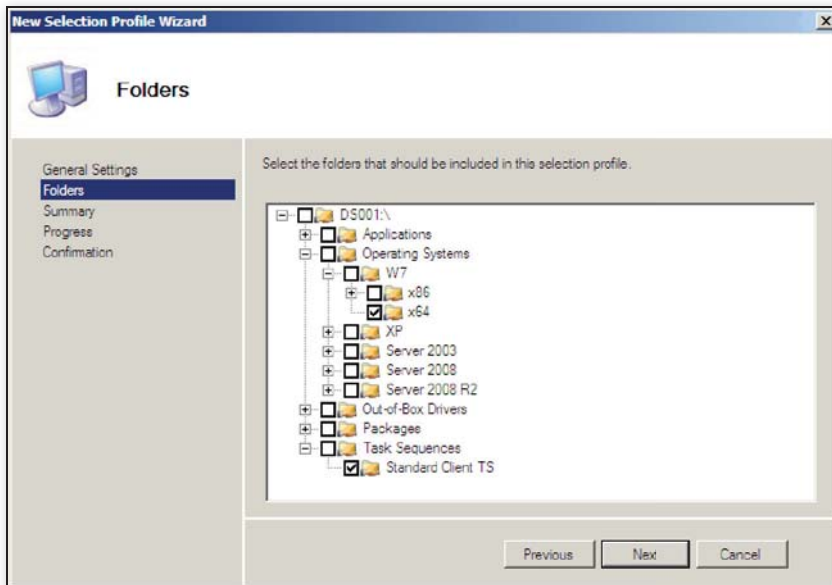


Figure 1: Selecting the MDT components for your selection profile

- The following folder structure, created in the deployment workbench:
Operating Systems\W7\x86, Operating Systems\W7\x64 (Windows 7's full set of source files reside here), and Task Sequences\Standard Client TS
- A task sequence, created in the Task Sequences\Standard Client TS folder with Task sequence ID=W7x64 and Name=Windows 7 64-bit (accept defaults, except you should provide an admin password)
- The updated deployment share (F:\DeploymentShare)

Step 1: Create Selection Profiles

Creating media requires the use of a selection profile. A selection profile lets you group MDT components (OS, applications, drivers, packages, and task sequences) into a single container. That selection profile is specified in the media, identifying which MDT components should be included. To create a selection profile from within the MDT's deployment workbench, follow these steps:

1. Expand the Advanced Configuration node.
2. Right-click Selection Profiles and choose New Selection Profile.
3. On the General Settings page, give the selection profile a name. (I named mine SAM—short for Stand Alone Media.) Input your comments to document what's included in this selection profile, then click Next.

4. On the Folders page, expand Operating Systems, then W7, and choose the x64 folder. Then expand the Task Sequences node and choose the Standard Client TS folder and click Next. The Folders page should look like Figure 1.

5. The Summary page lets you review your settings (make any changes necessary by clicking the Previous button). When you're done, click Next. The Progress page flashes by and then the Confirmation page appears. Click Finish on the Confirmation page.

Step 2: Create Media

Once you have a selection profile, you can create your new media. To create media from

within MDT 2010's deployment workbench, follow these steps:

1. From the Advanced Configuration node, right-click Media and choose New Media.
2. The New Media Wizard opens to the General Settings page. In the *Media path* field, type the folder name where you'd like to store the new media (the folder must already exist—MDT won't create it for you) or click Browse and navigate to a folder. I navigated to the F drive, where I created a new folder named SAM. (The selection profile name and media name don't have to match, but I've found that after you have a few of each, it's easier to track if they do.) Click OK, then input your comments and choose the SAM selection profile you created earlier from the drop-down list, as seen in Figure 2.

3. Review your settings on the Summary page. If all looks good, click Next. The Progress page shows the steps performed to create the new media; it disappears when completed. The Confirmation page appears. Click Finish to end the New Media Wizard.

4. The new media will be displayed in the Details pane of the deployment workbench named MEDIA001. (You can rename MEDIA001 just like you rename a file in Windows Explorer.)

Step 3: Update Media

Now that you've created the media, you'll need to update the media to generate a bootable ISO image containing your media. Before you update the media content, be sure you have enough hard drive space to

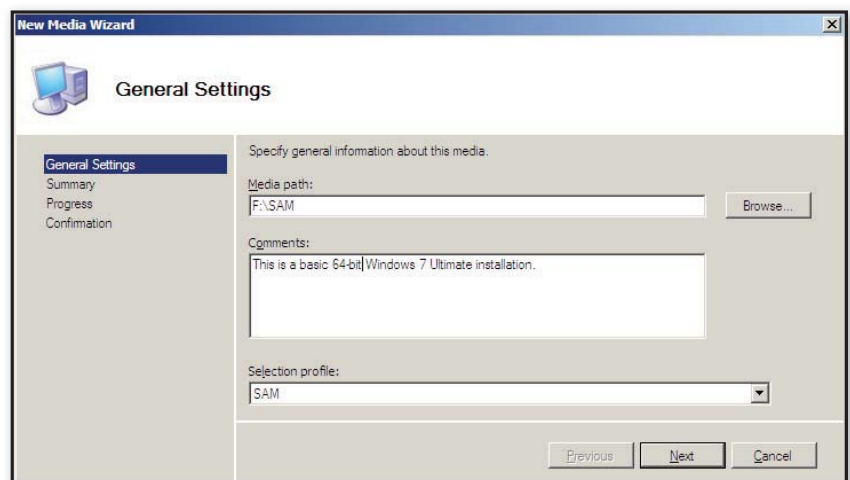


Figure 2: New Media General Settings page

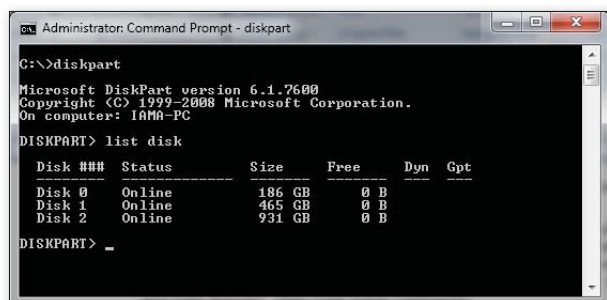


Figure 3: Results of DiskPart list disk command

store the new .ISO file. The Update Media Content Wizard doesn't check for available hard drive space before it generates the Lite Touch bootable .ISO file, so you can run into trouble if there isn't enough space to store it. The size of the .ISO file is determined by which MDT components you've included in your selection profile. You should be safe with at least 10GB available. To update the new media from within the deployment workbench, follow these steps:

1. From the Advanced Configuration\Media node, right-click MEDIA001 (in the Details pane) and choose Update Media Content.
2. The Progress page displays the steps performed by the Update Media Content Wizard; when it's done, the Confirmation page appears.
3. Click Finish on the Confirmation page.

Updating media is somewhat different from updating a deployment share. When you update a deployment share, you see an Options page that lets you choose how you'd like to update the deployment share (update existing files or create all new). This page is lacking when you update media. I'll show you later how to force a new .ISO file to be created instead of updating the existing .ISO file, which is helpful if you ever have a corrupt .ISO file that needs to be rebuilt.

The Update Media Content Wizard generates a Lite Touch bootable ISO file named LiteTouchMedia.iso in the F:\SAM folder. Now that you have the LiteTouchMedia.iso file, what can you do with it?

Step 4: Prepare Media

Burning the LiteTouchMedia.iso file to a DVD is as easy as right-clicking the

.ISO file and choosing *Burn disc image* if the .ISO file resides on a Windows 7 machine. Otherwise you need to find .iso-burning software, such as the CDBurn or DVDBurn Resource Kit utilities. You can also put the media on a UFD or external hard drive,

but the steps are a little different. Preparing the external device requires formatting the hard drive or UFD, so be sure there's nothing on it that you want to keep. To put your LiteTouchMedia.iso file on a UFD or external hard drive, perform these steps on a Windows Vista or later OS (you'll need the DiskPart utility):

1. Open an elevated command prompt (right-click the command prompt and choose *Run as administrator*), then type diskpart.
2. At the DISKPART> prompt, type these commands:

```

List disk
Select disk <N>
clean
create partition primary
select partition 1
active
format fs=ntfs
assign
exit

```

where N is the number of the disk. Be sure to record the number of the external device in the Disk ### field; mine is Disk 2, as Figure 3 shows. Close the command prompt.

3. Your external device is now ready to copy the required files from your media. Open Windows Explorer and navigate to your Media folder's Content folder (mine was F:\SAM\Content). The Boot and Deploy subfolders need to be copied to the external device. But wait—you'll also need to copy the protected system files autorun.inf and bootmgr, which are hidden by default. If you don't see the protected system files in the F:\SAM\Content folder you'll need to change the View Properties for the folder. Edit the View Properties by first going to the

correct folder (F:\SAM\Content), then selecting *Folder and search options* from the Organize drop-down list.

4. From the Folder Options, View tab, clear the advanced setting's *Hide protected operating system files (Recommended)* check box. When asked if you're sure you want to display these files, click Yes and then OK.

5. Copy the entire contents of the F:\SAM\Contents folder (Boot and Deploy folders, autorun.inf, and bootmgr) to your external drive or UFD.

Now you're ready to test your new media. If you burned your LiteTouchMedia.iso file to a DVD, place the DVD in the drive and boot the machine, being sure to press a key when prompted to boot from CD/DVD. Testing your media from an external hard drive or UFD device can be more complex. The machine you want to boot the external device from must be capable of booting from an external hard drive or UFD. You might have to edit the system's BIOS to set it to boot from the external media. Editing the BIOS is different on various types of computers—on one computer you might have to press F2, whereas another might require pressing F1. However you access your boot options, make sure you've listed the external device as a boot option. Plug in the device and turn on the computer—it should boot directly from your media and offer you the following Media client experience.

Step 5: Use the Media on the Client

Whether booting from DVD, an external hard drive, or a UFD, the client experience is the same. Follow these steps to deploy your Windows 7 x64 OS image:

1. The first screen presented is the boot menu. By default, all media supports 32- and 64-bit platforms. Select LiteTouch Boot [MEDIA001] (x64) [EMS Enabled] and you'll see the *Welcome Windows Deployment Wizard*. From the Welcome page, you can select *Exit to Command Prompt*, which comes in handy for troubleshooting failed deployments. If you receive network errors, you can run an ipconfig command from the command prompt to ensure you have a valid IP address, subnet mask, and so on, or to review the logs generated by the MDT

deployment process. The logs can be found in different places depending on how far the deployment has gotten. Prior to creating the C volume and formatting it, the log files can be found in X:\MININT\SMSOSD\OSDLOGS. After the deployment process has created and formatted the C volume, you'll find the logs in C:\MININT\SMSOSD\OSDLOGS. Lite Touch deployment assumes you have a DHCP infrastructure. If not, or if you want to set static IP information, click the *Configure with Static IP Address* button. (If you configure your static settings and click OK, reopening that page will wipe everything clean, so no double-checking here.) You can force a reboot by clicking the Reboot button in the bottom left corner. The top selection is the one you want—click *Run the Deployment Wizard to install a new Operating System* to begin the deployment.

2. The *Select a task sequence to execute on this computer* page lists the task sequences available based on the platform you chose from the boot menu (x86 or x64). If you selected Litetouch Boot [MEDIA001] (x86) [EMS Enabled], only task sequences that deploy 32-bit OSs and task sequences that don't deploy an OS, such as the *Sysprep and Capture task sequence* are listed. (*Sysprep and Capture task sequence* syspreps a machine and creates a .wim image ready for deployment.) If you choose Litetouch Boot [MEDIA001] (x64) [EMS Enabled], the list of task sequences will include 32-bit and 64-bit task sequences along with task sequences that don't deploy an OS. Choose the Windows 7 64-bit task sequence you created while following along with last month's article, and click Next.

3. Give the computer a name on the *Configure the computer name* page, and click Next.

4. Join the machine to either a domain or a workgroup on the *Join the computer to a domain or workgroup* page, and click Next. You'll need to provide credentials if you're joining the machine to a domain.

5. If you've captured the user's settings and data and stored them in a network location, you can specify that location on the *Specify whether to restore user data* page (provide the UNC path\\ServerName\

SharedFolderName). If you didn't capture the user's settings and data, select *Do not restore user data and settings*.

6. On the *Language and other preferences* page, select your language, time and currency formats, and keyboard layout from the drop-down lists provided.

7. Select your time zone on the *Set the Time Zone* page.

8. Enter the password you would like for the local administrator password on the *Administrator Password* page.

9. The *Specify the BitLocker configuration* page lets you enable or disable BitLocker and choose where to store the BitLocker recovery key. Choose your level of security and click Next.

10. The *Ready to begin* page has a Details button that will show all the choices you made in the deployment wizard. If you'd like to make changes, click the blue circle with the back arrow in the bottom left corner to go back to the page you'd like to change. When you're ready, click the Begin button to start the deployment process.

Once the deployment has completed successfully you'll see the *Operating system deployment completed successfully* page. Mine took only 20 minutes, but your time might vary depending on the speed of your deployment server and target machine.

Step 6a: Customizing Your Media

Up to this point, I've shown you the default behavior for creating and deploying media. But what if you want to deploy only 64-bit images, or you'd like some (or all) of the pages in the deployment wizard to be automated? In this section, I'll show you how to customize the supported platforms (x86 and x64) and automate the deployment wizard.

As you've seen, the LiteTouchMedia.iso file supports 32-bit and 64-bit OS deployments. This is done by providing two Windows Preinstallation Environments (WinPEs) in the LiteTouchMedia.iso file. You can customize these WinPEs by choosing specific types of drivers (e.g., network, video, mass storage) and optional fonts (such as Chinese, Japanese, and Korean) to be included. You can also create a Lite Touch bootable .ISO image that contains only a 32-bit WinPE or a 64-bit WinPE.

Providing support for only one platform reduces the size of the .ISO image, though not by much, and speeds up the boot process because when you have only one WinPE, there's no boot menu—it simply boots into the only available WinPE.

To create a Lite Touch bootable ISO image that supports only 64-bit image deployments, you'll need to edit the default properties of your media (MEDIA001). To edit the properties of MEDIA001 from within the deployment workbench, follow these steps:

1. Expand the MDT Deployment Share\Advanced Configuration node and highlight Media.

2. In the Details pane, double-click MEDIA001 (or right-click and choose Properties). The Properties window of MEDIA001 has six tabs.

3. The General tab shows *Media identifier* (media name), Comments, and Media path, all of which are read-only fields. Both platforms (x86 and x64) are selected by default. To create a 64-bit-only Lite Touch bootable ISO image, remove the checkmark from the *Generate x86 boot image* box. Give the new Lite Touch bootable ISO image a name (I named mine LTM64.iso) and click OK.

4. Next you'll need to update your media. In the Details pane, right-click MEDIA001 and choose Update Media Content. When the Media is updated, click Finish (this can take a few minutes).

Creating a 32-bit Lite Touch bootable ISO image is performed the same way; just de-select *Generate x64 boot image*, give it a new name, and update MEDIA001. I'm giving each Lite Touch bootable ISO image a new name because once you've generated a Lite Touch bootable ISO image, it can't be modified to support different platforms. Therefore, it's best to select your supported platform before you update MEDIA001. If you must make a change after you've updated MEDIA001, you can either create a new Lite Touch bootable ISO image by giving it a new name or delete the original LiteTouchMedia.iso file from the F:\SAM folder. The new Lite Touch bootable ISO image file will be created in the F:\SAM folder.

```
[Settings]
Priority=Default
Properties=MyWonderfulDeployment

[Default]
OSInstall=Y
SkipTaskSequence=YES
TaskSequenceID=W7x64
SkipComputerName=YES
ComputerName=Marketing1
SkipDomainMembership=YES
SkipUserData=YES
SkipProductKey=YES
SkipCapture=YES
SkipLocaleSelection=YES
KeyboardLocale=En-US
UserLocale=En-US
UILanguage=En-US
SkipTimeZone=YES
TimeZoneName="Eastern Standard Time"
SkipAdminPassword=YES
AdminPassword=P@ssw0rd
SkipBitLocker=YES
SkipSummary=YES
```

Figure 4: Example Rules tab settings for a fully automated installation

You can modify your x86 and x64 WinPE settings, such as the drivers and language packages that are injected into your WinPE. If you chose to support only x86, the Windows PE x86 Settings and Windows PE x86 Components tabs are what you'll want to configure. If you chose to support only x64, you'll want to configure the Windows PE x64 Settings and Windows PE x64 Components tabs. The settings and components tabs for each platform are identical; they simply pertain to their specific platform. The settings tabs let you configure a custom background or size of the scratch space (scratch space is used as temporary storage space in RAM). The components tabs let you choose a specific selection profile that contains drivers and packages to inject into your WinPE. The default selection profile is *All Drivers and Packages*, but you can streamline this by selecting the types of drivers you want injected. The four types are network, mass storage, video, and system-class drivers.

The Rules tab contains a list of settings that dictate which pages of the deployment wizard appear and which don't appear during the deployment process. The settings in this tab are stored in the file `F:\SAM\Content\Deploy\Control\CustomSettings.ini`. The default settings are the following:

```
[Settings]
Priority=Default
Properties=MyCustomProperty

[Default]
OSInstall=Y
SkipAppsOnUpgrade=YES
SkipCapture=YES
SkipAdminPassword=NO
SkipProductKey=YES
```

The Rules tab also has an Edit Bootstrap.ini button in the bottom right corner. Clicking this button displays the following:

```
[Settings]
Priority=Default

[Default]
```

This file is read by the MDT deployment wizard to locate the root of a deployment share—but you're not using a deployment share, right? I'll show you how we can use the Bootstrap.ini file (`F:\SAM\Content\Deploy\Control\Bootstrap.ini`) to help in automating your media.

Step 6b: Automating Your Media

Automating your media lets you decide which pages of the deployment wizard are displayed and which are not. You automate media by editing the Rules tab (or the CustomSettings.ini and Bootstrap.ini files). To fully automate your deployment so someone need only boot from the DVD or other media, follow these steps from within the deployment workbench:

1. Expand the MDT Deployment Share\Advanced Configuration node and highlight Media.
2. In the Details pane, double-click MEDIA001 or right-click and choose Properties.
3. Click the Bootstrap.ini button and add the new line `SkipBDDWelcome=YES` like this:

```
[Settings]
Priority=Default

[Default]
SkipBDDWelcome=YES
```

Close Bootstrap.ini, saving your new settings. To completely automate the deployment wizard, change the Rules tab to look like Figure 4.

There's a lot more you can do with automated settings, such as joining your target machine to a domain. To join a machine to the Deploy.com domain using the Rhonda user account (which only has permissions to join machines to the domain and create computer objects—it's not a domain admin account) with a password of P@ssw0rd and storing the newly created computer object in the Workstations OU (that you created), you would add the following settings:

```
SkipDomainMembership=YES
JoinDomain=Deploy
DomainAdmin=Deploy\Rhonda
DomainAdminPassword=P@ssw0rd
MachineObjectOU=OU=Workstations,
DC=Deploy,DC=Com
```

For a complete listing of all settings that can be automated, refer to the MDT 2010 documentation's "Microsoft Deployment Toolkit Reference—Providing Properties for Skipped Windows Deployment Wizard Pages," which is accessible by clicking Help in MDT. As you become more familiar with MDT 2010, you'll probably be creating and deleting a lot. I'd like to make one more point on deleting media. Deleting media only removes the media from the deployment workbench. The complete folder structure (along with the Lite Touch bootable ISO image created) doesn't get deleted. So if you delete media and wish you hadn't, just right-click the Media node and choose New Media. In the Media path field, click the Browse button and navigate to the old folder. Then choose the selection profile from the drop-down list, click Next twice, and click Finish on the Confirmation page. You'll be ready to go again in no time.

I hope this article helps you get a little more familiar with the Media function provided in MDT 2010.



InstantDoc ID 104644



Rhonda Layfield

(rhonda@minasi.com) is a consultant, trainer, Setup and Deployment MVP, and desktop deployment product specialist.

Create Active Directory MMC Consoles for Down-Level Administrators

After you have fully implemented a least-privilege delegation model in Active Directory, I recommend that you take the next logical step, which is to provide administrative tools that make it as easy as possible for administrators to perform the tasks they have been delegated. This is particularly important for front-line administrators, who are typically less familiar with Active Directory and with the specific procedures of your organization. By creating productive MMC consoles, you can provide visibility to tasks, tools, and documentation that will empower your administrative teams. The consoles will consist of taskpads, and the taskpads will quite often be derived from saved queries rather than from organizational units or containers in the Active Directory hierarchy. Integrate procedural documentation directly into the console, along with an administrative home page that can serve as both the opening page of the console and the hub for navigation to each taskpad.

Empower your
administrative
team

by Dan Holme

Create a Console with Saved Queries

First, open a blank MMC and add the Active Directory Users and Computers snap-in. Although you can create taskpads using your OU structure, you will be better served by creating saved queries.

Saved queries are, in my opinion, the foundation for effective administration in the Active Directory Users and Computers snap-in. You can create saved queries that display views of objects based on the scopes of management for your administrators. For example, for your Help Desk you can create views of all nonadministrative users, all client computers, and all groups. For a team that supports users in a particular site or department, you can create views that show the users and computers in that scope of management based on those objects' membership in a relevant group.

When you create a saved query for user objects, I recommend adding the pre-Windows 2000 logon name as a column because many of the tools and scripts in this resource kit can be added as taskpad tasks and pass the pre-Windows 2000 logon name as a parameter. Figure 1 shows a saved query that displays all nonadministrative users in the domain.

Create a Taskpad with Tasks for Each Delegated Ability

Next, for each saved query, create a taskpad view with tasks for the capabilities that you have delegated to the team that will use the console. For example, if you have delegated the ability to reset user passwords, provide a task for the Reset Password menu command. The following steps summarize how to create a taskpad view for a saved query displaying user objects:

1. Right-click the saved query that displays the objects for which you have delegated administrative tasks, and choose New Taskpad View.
2. The New Taskpad View Wizard appears. Click Next.
3. In the Taskpad Style page, click Next.
4. In the Taskpad Reuse page, select the Selected Tree Item option button and click Next.

Editor's Note

*From Windows Administration
Resource Kit: Productivity Solutions
for IT Professionals*

By Dan Holme

Publisher: Microsoft Press

Released: February 2008

Pages: 752

[http://www.microsoft.com/
learning/en/us/book.aspx?
ID=11297](http://www.microsoft.com/learning/en/us/book.aspx?ID=11297)

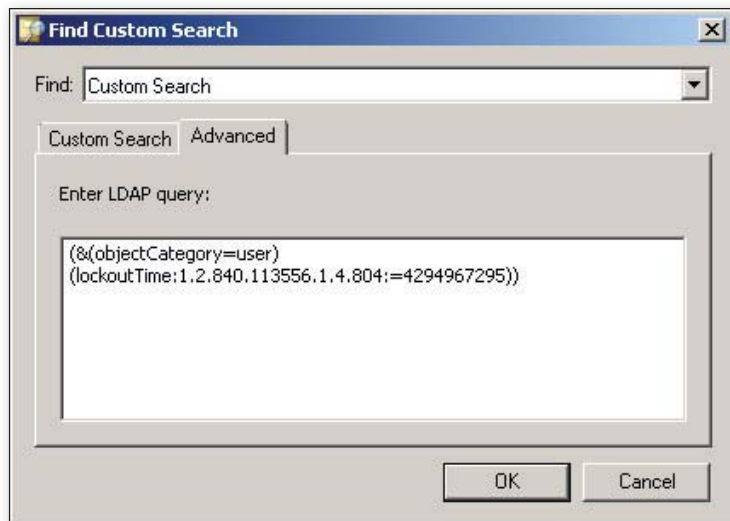


Figure 1: A saved query showing all nonadministrative users as the basis for a taskpad

5. In the Name And Description page, accept the default name and click Next.

6. Clear the Add New Tasks To This Taskpad After The Wizard Closes check box, and click Finish.

After you create the taskpad view, add tasks for each delegated ability. When adding tasks for commands such as the Reset Password command, you add menu command tasks. The following steps illustrate the process for adding menu command tasks:

1. Right-click the saved query for which you created the taskpad, and choose Edit Taskpad View.
2. Click the Tasks tab.
3. Click the New button.
4. The New Task Wizard appears. Click Next.

5. Select the Menu Command option button, and click Next. The Menu Command page appears, as shown in Figure 2.

6. Select a command from the Available Commands list. The list of menu commands in the Available Commands list is based on the type of object selected on the left side of the dialog box. This is one of the trickiest and most frustrating parts of building taskpads. For example, notice in Figure 2 that the Disable Account command is available but there is no Enable Account command. That's because the selected object is an enabled user. If you select a disabled user on the left side, the Enable Account command appears but the Disable Account command disappears. So you must select

the correct type of object before the command you want becomes available.

7. Click Next.

8. Enter the name for the task in the Task Name box. This name will be the label of the hyperlink to the task.

9. Optionally, enter a description in the Description box. This description will appear below the task hyperlink in the taskpad.

10. Click Next.

11. Select an icon or click the Custom Icon option button, and then click Browse to choose an icon. There are more interesting and colorful icons in the file C:\Windows\System32\Shell32.dll. Windows Vista and Windows Server 2008 also have a plethora of icons in C:\Windows\System32\Imageres.dll.

12. After you have selected your icon, click the Next button.

13. Click Finish, and then click OK to close the Properties dialog box for the query you selected.

The resulting taskpad should appear similar to Figure 3. I added several more tasks. Remember that tasks are context sensitive—the tasks you've added to the taskpad appear only when you select an object in the details pane.

Add Productive Tools and Scripts to the Taskpads

Make sure to integrate into the taskpads links to useful tools and utilities from Microsoft from the *Windows Administration Resource Kit* and from third parties. Also add shell commands that can launch common applications such as the command prompt. The administrator who uses this console will log on to her system with a nonprivileged user account. She will then proceed to launch this console with the elevated credentials of her administrative account. Any processes launched from the console will inherit elevated credentials, allowing easy access to administrative tools without the need to reenter the secondary user name and password.

Add Procedures and Documentation to the Console

I recommend that you integrate documentation of your environment and of procedures related to Windows administration directly



Figure 2: The Menu Command page of the New Task Wizard

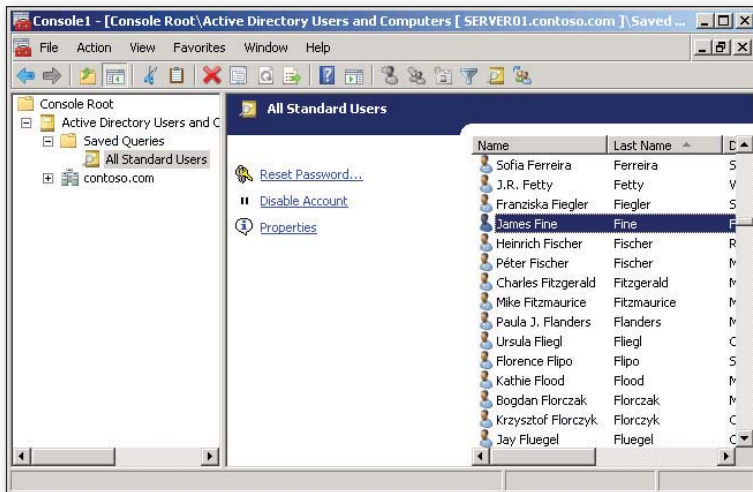


Figure 3: A taskpad and tasks

into the MMC. This can be done one of two ways. First, you can add a shell command task to a taskpad that launches a document with the appropriate application. For example, a shell command can launch `winword.exe` with a parameter that opens procedural documentation. Second, if the documentation is available on your intranet, you can integrate the documentation using a Link to Web Address snap-in.

Create an Administrative Home Page within the Console

Create a node in the console that can be used as a home page for the console. Because of the awkward way in which navigation between taskpads is implemented, you will find it much easier to have this home page as a kind of home base or hub from which you can navigate to individual taskpads. Each task will have a single navigation link back to this page.

You can use any taskpad as this home page, but if you happen to have an intranet site for your administrators, such as a SharePoint or IT portal, I suggest you add that into the MMC using a Link to Web Address snap-in and then create a taskpad using that snap-in. A folder snap-in can serve as a home page if you use a taskpad with the *no-list* format.

At one client location where we leveraged such consoles, the administrative home page of the MMC was a taskpad for a Link to Web Address snap-in, which itself pointed to the home page of our IT administration SharePoint site. SharePoint then allowed us to easily manage Web

content that was then integrated directly into the console. For example, we included a schedule of help desk shift assignments and important announcements on the SharePoint home page so that information was regularly visible to administrators as they navigated between taskpads.

Add Each Taskpad to the MMC Favorites

Navigate to each taskpad in the console that you want to make available to the administrators who will use the console. Add the node to your Favorites in the console using the Favorites menu. Be sure to add the administrative home page to your Favorites folder as well.

Create Navigation Tasks

Edit the taskpad view of the administrative home page, and add navigation tasks to each of the nodes that you added to your Favorites folder. Then edit each taskpad, and add a single navigation link back to the administrative home page. After you have completed these steps, you should be able to use the navigation tasks on each taskpad to navigate between the administrative home page and each taskpad in the console.

Figure 4 shows an example of the resulting administrative home page. Each of the other taskpads in the console can be reached using navigation tasks on the left-hand side of the taskpad.

Save the Console in User Mode

To prevent users from modifying your task pad, you need to save the console in User mode. To change a console's mode, choose File, Options. By default, new consoles are saved in Author mode, which enables users to add and remove snap-ins, view all portions of the console tree, and save customizations. User mode, on the other hand, restricts the functionality of the console so that it cannot be changed. There are three types of user modes, described in Table 1. User Mode—Full Access is commonly selected for a console provided to skilled administrators with diverse job tasks requiring broad use of the console's snap-ins. User Mode—Limited Access is a locked-down mode and

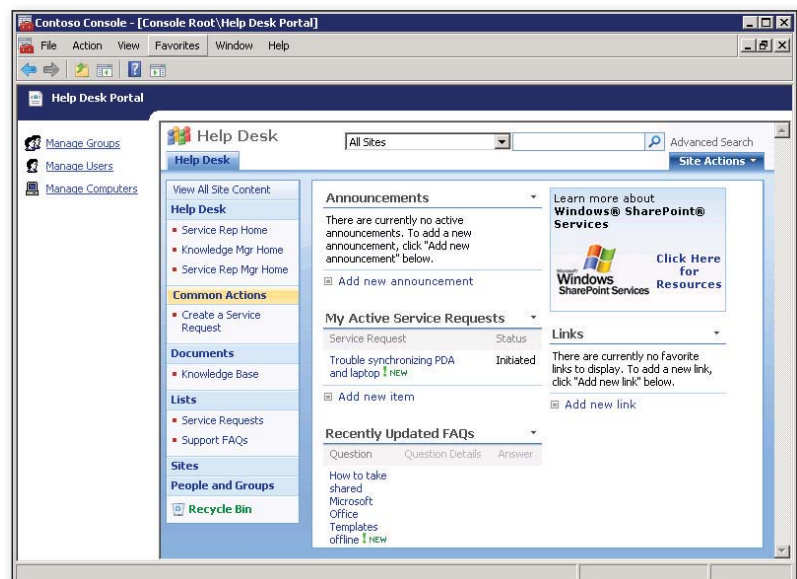


Figure 4: An Intranet site exposed in a taskpad view of a Link to Web Address snap-in acts as the hub for the console, using navigation tasks

■ ACTIVE DIRECTORY MMC CONSOLES

Table 1: MMC Modes

Mode	Use when
Author	You want to continue customizing the console.
User Mode—Full Access	You want users of the console to be able to navigate between and use all snap-ins. Users will not be able to add or remove snap-ins, or change the properties of snap-ins or the console.
User Mode—Limited Access, Multiple Windows	You want users to navigate to and use only the snap-ins that you have made visible in the console tree, and you want to preconfigure multiple windows that focus on specific snap-ins. Users will not be able to open new windows.
User Mode—Limited Access, Single Window	You want users to navigate to and use only the snap-ins that you have made visible in the console tree, within a single window.

is therefore selected for a console provided to administrators with a more narrow set of job tasks. When a console is no longer saved in Author mode, you—the original author—can make changes to the console by right-clicking the saved console and choosing Author.

Lock Down the Console View

This last step enables you to lock down the console completely. If you click the View menu and choose the Customize

command, you can choose to hide some or all of the components of the MMC window. By hiding the console tree, for example, you discourage administrators from browsing the directory by restricting them to the taskpads and navigation links you have provided.

Distribute the Console

Save the highly customized console to a location that can be accessed by all administrators. That will make it easier for

you to manage revisions to the console. Remember that consoles are basically a set of instructions that are interpreted by mmc.exe—instructions that specify which snap-ins to add and which computers to manage with those snap-ins. Consoles do not contain the snap-ins themselves. Therefore, a console will not function properly if the snap-ins it contains have not been installed. So be sure you have installed appropriate snap-ins from the Administrative Tools (adminpak.msi in Windows XP and Windows Server 2003) or the remote server administration tools (RSAT in Windows Vista or Windows Server 2008).

InstantDoc ID 103678



Dan Holme

(danh@intelliem.com) is director of consulting at Intelliem, which delivers solutions-focused training and consulting services supporting enterprise SharePoint, Office, Windows, and Active Directory implementations.

SharePointPro CONNECTIONS

Hone your skills with SharePoint tips and tricks, product reviews, and solutions you'll find in the all new *SharePointPro Connections* magazine. Sign-up today and you'll get a print subscription (4 issues) FREE!

Upcoming articles include:

- Migrating to SharePoint 2010
- Using SharePoint with Visual Studio
- Getting more out of SharePoint

Limited number of free print subscriptions available so **ACT NOW!**

www.sharepointproconnections.com/subscribe.aspx





What You Need to Know in a Mixed 32-bit and 64-bit Environment



In the past year, I have helped several clients make the transition from a 32-bit Windows environment to a mixed environment of 32-bit and 64-bit Windows. After the transition, several observant end users pointed out an “oddity” in their new 64-bit Windows systems that were running on Intel 64 processors. If you look at the `PROCESSOR_ARCHITECTURE` environment variable from the Control Panel’s System applet or from 64-bit `Cmd.exe`, its value is *AMD64*.

Although the value might appear to specify the wrong vendor (AMD instead of Intel), the value is what it should be. `PROCESSOR_ARCHITECTURE` is about the architecture and not the implementation. Because the Intel 64 processors implement the AMD64 architecture, they’re members of the AMD64 processor class.

I’m not pointing this out to you as a curious fact. From an IT support perspective, processor architecture means Windows architecture, and multiple Windows architectures in an organization means multiple versions of everything from Windows source files to service packs to drivers. Understanding processor architectures can help you untangle some of the problems you might encounter in a mixed 32-bit and 64-bit network environment. Therefore, I’ll discuss all three current processor architectures—x86, IA64, and AMD64—although I’ll be calling them Windows architectures. Then, I’ll point out a few other things to watch out for when you transition to a mixed 32-bit and 64-bit Windows environment.

x86

The x86 Windows architecture is the only remaining 32-bit non-embedded Windows architecture. Naturally, it runs on all processors implementing the x86 processor architecture. However, there are a couple of important caveats to keep in mind when Windows tells you it is x86 Windows.

The first caveat is that the AMD64 processor architecture is a superset of the x86 processor architecture, so the x86 Windows architecture can run on the AMD64 processor architecture. The bulk of computers shipped during the past five years running x86 Windows are actually running on 64-bit processors. Although you can’t directly upgrade these installations to 64-bit Windows, it’s quite possible to perform a clean 64-bit Windows installation on them.

Although there’s no way to directly tell that 32-bit Windows is running on a 64-bit processor, you can use the built-in Windows Management Instrumentation Command-line (WMIC) utility to check the processor’s name easily enough, after which you can check the processor’s capabilities with the manufacturer. To check the processor name on the local machine, open `Cmd.exe` and run the command

```
wmic cpu get name
```

Understanding processor architectures is key

by Alex K. Angelopoulos

■ MIXED ENVIRONMENT

If you want to check the processor name on a remote computer named x51, you'd run the command

```
wmic /node:x51 cpu get name
```

The second caveat is that 64-bit Windows platforms will also run 32-bit x86 Windows applications in a special x86 Windows emulator. Even though the Windows OS itself is 64-bit, within the emulator, Windows looks exactly like it's x86 Windows. Part of what "exactly" means is that the `PROCESSOR_ARCHITECTURE` variable's value is x86. You can still tell what the real environment is, though. The x86 emulator also exposes a variable named `PROCESSOR_ARCHITECTURE_W6432` that contains the architecture for Windows itself. If the variable doesn't exist, you're running on x86 Windows all the way down to the hardware.

You can also use WMIC to check the real value of `PROCESSOR_ARCHITECTURE`. For example, to check the true architecture of the local computer and the x51 remote computer, you'd run the commands

```
wmic environment where  
    "name='PROCESSOR_ARCHITECTURE'" get  
and
```

```
wmic /node:x51 environment where  
    "name='PROCESSOR_ARCHITECTURE'" get
```

respectively. (Although these commands wrap here, you'd enter each command on one line.)

Every Windows version since the beginning of the Windows NT family has supported the x86 architecture, but that's about to change. Although Windows 7 supports x86 architectures, Windows Server 2008 R2 is x64 only.

IA64

AMD wasn't the only one to design a 64-bit processor architecture. Intel designed a 64-bit processor architecture named IA64. The first modern 64-bit Windows was designed to run on processors implementing the IA64 architecture. Therefore, it has a native `PROCESSOR_ARCHITECTURE` of IA64. The only processor families that implement IA64 are Intel's Itanium and Itanium 2. Only the

Windows Server platforms currently support IA64. Although Windows XP initially supported IA64 architecture, issues with legacy support kept IA64 processors from becoming more than a rarity on desktops. Microsoft dropped support for IA64 in XP in 2005.

AMD64

When Intel decided to drop backward compatibility with x86 processors with the IA64 architecture, AMD began work on an alternative 64-bit processor design that extended the x86 design in a backward-compatible fashion (just as the original Intel 80386 processors maintained compatibility with 80286 processors). AMD initially referred to the specification as x86-64, then renamed it AMD64. Microsoft's 64-bit versions of Windows built to run on this architecture also use the AMD64 name. Since the 2003 release of AMD64 XP, every release of Windows has supported the AMD64 architecture.

VIA Technologies and Intel sell processors that use the AMD64 architecture. For marketing purposes, Intel refers to the technology as Intel 64, obscuring the fact that its processors implement the AMD64 instruction set. Similarly, Microsoft has begun using the name x64 for this architecture to minimize confusion about the correct Windows architecture. Whatever the marketing name, the Intel 64 processors run precisely the same Windows builds as any other processors implementing the AMD64 architecture. In terms of the Windows versions and Windows software supported, you can treat the terms AMD64, Intel 64, x86-64, x64, and the less-known EM64T as roughly equivalent.

Other Things You Should Know

The last significant platform migration affecting the entire IT world occurred in the 1990s, when desktops moved from 16-bit Windows and MS-DOS to 32-bit Windows. The move from 32-bit to 64-bit Windows is much simpler. Network management is more centralized than it was in the 1990s, and most activities are abstracted from OS bitness.

Even though the move from 32-bit to 64-bit Windows won't be as difficult as the last significant platform migration, here are some pointers to help you avoid common pitfalls:

- **Know software math—16 doesn't go into 64.** Users won't be able to run 16-bit software from a 64-bit Windows OS, so you should eliminate any 16-bit software hanging around from the 1990s. If a user needs to occasionally run 16-bit software (e.g., a legacy financial package to access old data), you could provide the user access to a 32-bit platform. If you have multiple users who need to run 16-bit software occasionally, you might consider running the software on a 32-bit terminal server. Another option is providing a 32-bit virtual machine (VM). Virtualization might be the best alternative because VMs are highly portable.
- **Be aware that IA64 (Itanium) is special.** Windows systems using IA64 processor architectures can run IA64 Windows only. If you're repurposing existing IA64 systems, they naturally fall into a server role. The print server role could cause problems because these systems need IA64 printer drivers. The one long-term limitation on these servers is that there are fewer 64-bit applications available for IA64 Windows than for AMD64 Windows. However, IA64 will run 32-bit applications.
- **Understand the incompatibilities between 32-bit and 64-bit software.** The x86 Windows versions can't run 64-bit applications. AMD64 and IA64 Windows will run ordinary 32-bit software, but not within the same process. Since 64-bit applications can't use 32-bit binaries, 64-bit versions of software applications won't be able to load 32-bit add-ons or components. If you depend on 32-bit components, you need to use a 32-bit version of the application. This is one of the reasons that 64-bit Windows systems use 32-bit Internet Explorer (IE) by default; there's a huge installed base of 32-bit controls that vendors haven't ported to 64-bit.
- **Realize that moving from 32-bit to 64-bit is a migration, not an upgrade.** If you're planning to move existing PCs from 32-bit to 64-bit Windows, you can capture settings and files with tools such as Windows

Easy Transfer, but you can't perform an upgrade. You can't even run the 64-bit installation for a new Windows version from within 32-bit Windows. You must perform a fresh install of Windows.

- **Check your drivers.** You can't use 32-bit kernel-mode drivers on 64-bit Windows. The WOW64 subsystem is available only above the OS kernel. So, checking the drivers before you migrate from 32-bit to 64-bit is crucial.
- **Be ready to help users check their Windows architecture.** The Windows look and feel is identical across the 32-bit and 64-bit computing lines, so users might not know whether they're on a 32-bit or 64-bit OS. IT support staff should be ready to walk end users through verifying their Windows architecture when problems arise. The Microsoft article "How to determine whether a computer is running a 32-bit version or 64-bit version of the Windows operating system" (support.microsoft.com/kb/827218) can serve as a conversational script for telephone support, or the link to the article can be sent to users.

What You Need to Remember

Although the move from 32-bit to 64-bit computing won't be simple (particularly when complicated by end-user confusion about names), it's unlikely to be an overwhelming hardship. The identical UIs across platforms and the support for existing 32-bit software make most of the change transparent. The fact that 64-bit Windows versions use 32-bit IE by default also helps make the change transparent. (If this wasn't the default, the calls about Adobe Flash Player not running in web pages alone could bring the average Help desk to its knees.) The dual IA64 and AMD64 architectures aren't a significant problem either. IA64 is generally used in high-end roles, where the lack of support for specific hardware and software can be considered a feature rather than a problem.

The most important points for the move to 64-bit computing come down to the following. Before you migrate a computer to 64-bit Windows, you need

to make sure it has 64-bit drivers and eliminate (or make special arrangements for) any 16-bit software. To perform the migration, you must perform a fresh install—you can't upgrade. Finally, make sure IT support staff can help users determine whether they're running 32-bit and 64-bit when problems arise. Although this migration isn't trivial, it pales in comparison to the work that was involved

in getting Windows 3.11 off the corporate desktop.

InstantDoc ID 103547



Alex K. Angelopoulos

(aka@mvp.org) is an IT consultant, an MCSE, and a contributing editor for *Windows IT Pro*. As an avid scripper, he regularly writes about administrative automation using WSH, PowerShell, and related technologies.

Prime Your Mind

with Resources from Left-Brain.com

Left-Brain.com is the online superstore stocked with educational, training, and career-development materials focused on meeting the needs of IT professionals like you.

Featured Product:

VMware vSphere Training

VMware vSphere Training courseware is appropriate for both new VMware administrators and those who are preparing for the VCP certification. Besides completely covering how to administer a VMware infrastructure, this course also reviews third-party solutions that are widely used by the virtualization community. Find out more about this course and other virtualization resources at Left-Brain.com

windowsitpro.com/go/left-brain/vsphere

*Plus shipping and applicable tax.



www.left-brain.com

WindowsIT Pro



InfoPath 2010 with SharePoint 2010: A Walkthrough

Design and create
a data-collection
form from the
ground up

by Ryan Thomas

InfoPath is a versatile data-collection tool designed to make the creation of forms within SharePoint extremely easy, efficient, and connected to out-of-the-box or custom workflows. And yet, for IT pros and even SharePoint developers, InfoPath remains a mysterious application. Because SharePoint adoption is steadily increasing, I want to pull back the veil to show you how you can integrate InfoPath forms in your SharePoint environment without the need for coding.

In “Solve Common Business Problems with InfoPath and SharePoint” (InstantDoc ID 103462), I discussed the benefits of combining InfoPath with SharePoint. In this article, I’ll dig a little deeper, showing you how to build a form from the ground up, using InfoPath 2010 Beta 2 and SharePoint 2010 Beta 2. As I walk through some examples, I’ll also point out ways to enhance certain components or functionality *with* custom code.

Getting Your Feet Wet

First, you’ll want to use InfoPath 2010 to create your first form. I want to focus mostly on InfoPath, so I won’t spend too much time on the SharePoint infrastructure; however, I’ll cover some of the SharePoint 2010 requirements where necessary. To get started, open InfoPath 2010 and click File, New from the top Ribbon.

Select the SharePoint Form Library template, then choose *Design this Form* in the navigation pane. You’ll see a new form in the design window with a basic-looking table from which to add labels and controls. To start, we’ll create a lightweight expense report form to illustrate how quickly you can begin to gather data into SharePoint.

Within the designer, you can select a color scheme under the Page Design tab. Remove the unwanted rows and add some quick labels to get the form to look bland and ready to have controls added to it, as Figure 1 shows.

Place your cursor in the table cell to the right of the Date cell, and from within the Home tab select the Controls menu item. Within this menu, select the DatePicker control. You should see a new DatePicker control added to your design surface where your cursor was placed, and a new XML element added to your Fields box on the right. These fields represent the data you’ll capture and their associated type. If you right-click the DatePicker control and select Properties, you can set formatting rules and supply a more readable name for the underlying data it represents. As you add more controls, you’ll get a growing XML

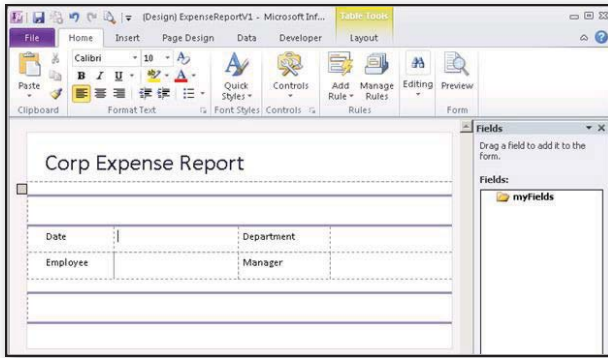


Figure 1: Ready for controls

container file ready to capture your form data in a standard format.

When adding data elements and associated controls, you should strongly consider giving your data the correct type (e.g., numeric, text, date, Boolean) and applying specific formatting and rules for these controls—anything from enforcing currency formatting to complex functions such as using XPath to evaluate other data elements to enable or disable controls based on the value of one or more other controls within your form. Doing so can add significant options.

I've filled out the design surface with some additional controls to show you what a basic expense report might look like. InfoPath provides much more extensive options for additional rules, formatting, and connectivity to additional data sources for querying and for creating business logic within your form. In the case of expense reports, you might want to query your SharePoint lists or SQL Server databases to obtain employee department and manager information automatically, mileage rates, per-diem amounts, and so on. This can easily be included to make more dynamic and flexible forms. Figure 2 shows a rudimentary expense report form. (I added a repeating table with some additional data collection to account for a varying number of expense items that can be filled out by end-users.)

Repeating tables are powerful within InfoPath. They represent something that competing options don't offer: easily capturing any number of user-defined records at run time while still maintaining all your rules, formatting, and functions. In other applications that designers use to collect data (e.g., Microsoft Excel, Word, ASP.NET), creating

manage the code to iterate over all the submitted record. InfoPath manages this data very easily because it knows in advance that there might be any number of rows within a group (XML Nodes). Most of the rules and formatting are automatically applied to each new row as it's created and filled out.

Publish Your Expense Report

If you would like to examine your XML container file, you can use the File menu in InfoPath and choose Publish, Export Source Files. Doing so will export the InfoPath package from an XSN file into native components. If you open these files, you can begin to make some sense of how InfoPath is packaged and designed. Under the covers, it's basically an XML schema definition, XML template, an XSL stylesheet (used to create your display elements), and an associated XSF file, which is a proprietary InfoPath file used to apply the rules, datasource details, and other native functionality.

If you feel particularly daring, you can make modifications to these files manually and repackage them into your XSN file. If you ever want to venture into building InfoPath forms in Visual Studio to add compiled code, this becomes very easy. Some of the potential benefits include copying and pasting rules for faster and less risky reuse, assigning property promotion to SharePoint via specific Site Columns in advance, and understanding how rules and data sources are applied. Although this is an advanced topic, it's important to know how the

an "add another item" for the user can be very frustrating within a single form. Excel has difficulty with using functions in named ranges when it doesn't know how many rows it must account for; ASP.NET forms must create the new row in code and then be specifically built to

files are put together in case you ever need to crack them open.

With a basic expense report form built, we're now ready to publish and use it inside SharePoint 2010. The first necessary action is to perform a design check to ensure that the form we've built can properly function within InfoPath Form Services. These services, native to SharePoint, can convert your InfoPath form into a fully functional web page by simply publishing the form to SharePoint. Select File, Info, Design Checker. In the Design Checker window, click the *Change settings* link at the bottom. Choose Web Browser Form in the drop-down list, then type in the URL to the SharePoint site where you wish to publish the form. Then, click OK. Select the *Verify on server* check box, and click Refresh. A dialog box will inform you that the form is being checked against your server.

The Design Checker will be your friend as you design larger and more complicated forms, up until your form gets too big—at which point, it will abruptly cease to be your friend. It will time out when trying to convert and evaluate your form to make sure it can be properly converted to a web page. This was a major problem in InfoPath 2007, and I'm hopeful that a fix is in sight. Even if the checker times out, your form will still work in SharePoint. The best option is to disable the Design Checker when it begins to time out. As long as your forms aren't very large, you'll be told if you're attempting to use any InfoPath features that aren't supported with web forms.

The next step is to select File, Submit Options, and insert the path to your document library where you want to store the filled-out forms in SharePoint. In the File Name text box, you need to set something that will enforce unique values to ensure that

Figure 2: Rudimentary expense report form

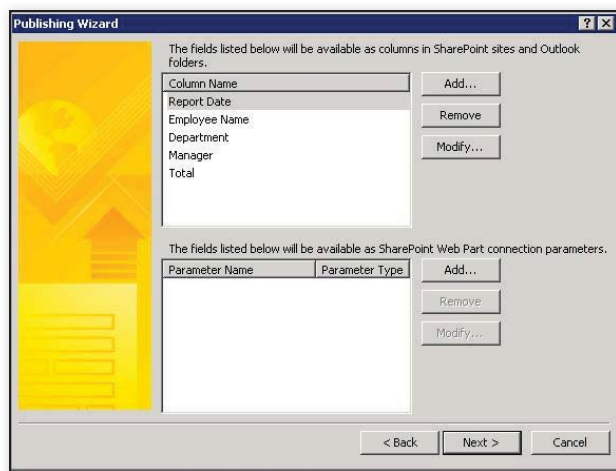


Figure 3: Sample test form

you don't have duplicate file names. There are many ways to do this, but for now I just used the date of the report with some text: `concat("Expense Report - ", ReportDate)`. Select Next, and choose a name for this data connection. This represents one way to quickly submit data to SharePoint, but you might find that you need to add submit buttons with more flexibility. For example, a button can run some rules and analysis on the data before allowing a submission.

The next step is to select File, Publish, *Publish form to a SharePoint Library*. Insert the URL to your SharePoint list and select Next. On the next page, ensure that you select the *Enable this form to be filled out by using a browser* check box. Choose the Site Content Type radio button, and select Next. By selecting this radio button, you're telling InfoPath that you want this form to be added as the template for a new SharePoint Content Type. On the following screen, select *Create a new content type* and select Next. Now, add a name and description for your new content type and select Next.

On the following page, you need to decide where to place this template so that it can be used by the new Expense Report content type. I usually like to put the template in a place where it can't be easily accessed. In this example, you can hide it in the list's Forms folder so that it will reside in your new form library but will be tough to readily find. (Here's where I placed mine: <http://2k8-sp2010-dev/Expense Reports/Forms/ExpenseReport.xsn>.)

The following screen is where you'll promote local fields in your InfoPath form to SharePoint lists as columns. Click the Add

button on the upper list. In the *Select a Field or Group* dialog box, select any fields in your form that you want to promote to SharePoint. In the *Site column group* drop-down list, select (*None: Create a new site column*). Below that, create a name for your new SharePoint column. This screen will enable SharePoint to automatically extract

data from your submitted forms to your SharePoint site columns with no additional effort. You will see this in action when you submit your first form shortly. Continue to add as many columns as you want. Figure 3 shows my test form.

For a more robust and reusable solution, you'll want to create your required site columns in advance within SharePoint. In that case, you can tell InfoPath to use them instead of creating new ones when publishing your form from within InfoPath. This becomes a powerful tool for collecting essential managed metadata from external sources and using custom search options in SharePoint to create a legitimate application around expense reporting or any other business process you might need to automate.

Now, you can continue through the remaining dialog boxes and publish your form. And you can browse to SharePoint to test your form. When you navigate to your form library, you must first disable the default form content type and add your new Expense Report Form content type. To do so, navigate to Library Tools, Library, Settings, Library Settings from within your Form Library. Click Advanced Settings, and ensure that the *Allow management of content types?* check box is selected. Then, navigate back to your Form Library Settings, and in the Content Types section, select *Add from existing site content types*, locate your new content type in the list box, and add it to your library. Return to

the previous page and in the Content Types section, click *Change new button order and default content type* and clear the Form box so that it doesn't appear in the list of available content types for this library when adding items.

When you're done with that, you can see your form in action by returning to the library and selecting Library Tools, Documents, New Document, Expense Report Form from the available document types. You should see your form in your browser window, as you see in Figure 4. (I've filled out some data to show what it can look like.) At the top of your screen, you should be able to submit the form and return to your SharePoint list.

Workflow

Now that you have a working expense report form, I'll walk you through the process of creating a workflow to allow submissions of expense reports to be approved by the accounting department. You'll use SharePoint Designer 2010 Beta 2 for this task.

Open SharePoint Designer and choose to open your site via the URL. After seeing your site information page, select Workflows in the left navigation. You'll see a list of workflows that already exist in your site. SharePoint 2010 now supports modifying the out-of-the-box workflows using SharePoint Designer 2010. In this case, you'll create a brand-new workflow for your expense reports. To see some new features in SharePoint Designer 2010, select Reusable Workflow from the Ribbon menu. SharePoint Designer 2010 can now create workflows that can be saved as templates and reused, or in this case attached to your Expense Report Form content type. Figure 5 shows the Create Reusable Workflow dialog box.

Date	Description	Category	Cost
2/1/2010	Fuel	Travel	\$45
2/2/2010	Lunch	Meals	\$23
2/3/2010	Cab Fare	Travel	\$37

Total: \$105

Figure 4: Viewing the form in your browser

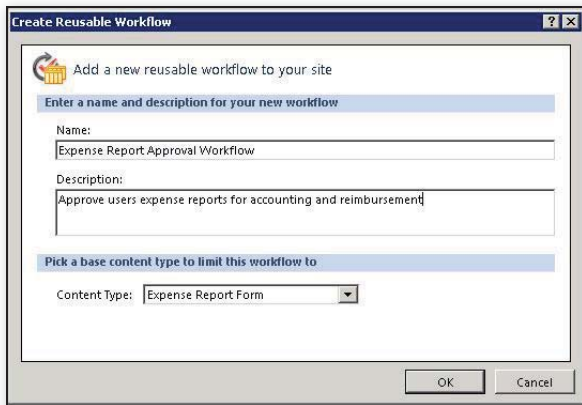


Figure 5: The Create Reusable Workflow dialog box

Select OK after you fill out the form. SharePoint Designer will connect to your server and create the shell for your new workflow. In the Ribbon, select Insert, Action, Start Approval Process. You'll see your new action appear in Step 1. Click Step 1 and rename it, for example, Expense Approval—something to help denote the intention of the step. Now, click the underlined *these users*. In the Participants field, you can put the user or group that will be assigned the approval task. In the Title field, you can click the ellipses to build a string with some dynamic values. In this example, I allowed for a duration of two days for the task. When you're done, click OK.

Now, you can save and click Publish in the Ribbon. Navigate back to your SharePoint site and to your Expense Report

list. In the Ribbon, click Library Tools, Library, LibrarySettings, Expense Report Form (*content type*), Workflow Settings, Add a Workflow. Select *Expense Report Form for the Content Type*, then select Expense Report Approval Workflow for your workflow template, and give your workflow a unique name. The rest of the settings can probably stay as defaults. I

ran into what I believe to be a beta problem that required me to click the Back button after selecting my content type (in order to select my custom workflow). Remember that some of these names might be different, depending on how you name your workflow and what content type is selected. When you're finished, click OK. Your workflow is now ready to run. To test the workflow, create a new expense report and select Workflows in the item's context menu.

On the Start a New Workflow page, you can select your custom workflow and click Start. Doing so should create an approval task for your accounting user. This user will have the option to approve, reject, reassign, and so on. Assuming he or she approves your report, you'll see an Approved link in the custom workflow column in your expense

report library. If you click on the link, you should see a screen similar to Figure 6.

This screen contains a lot of information, including any tasks created during this workflow, plus all the history data logged by the workflow process. There are some errors logged in my history because I didn't get email correctly configured in my test environment. You'll also notice another new feature at the top of the image: Visio Services. SharePoint Designer 2010 workflows can be exported and imported via Visio to provide a more robust and familiar design surface for workflow creation. These services automatically created a flowchart to depict my custom workflow. You'll see the benefits of this feature as your workflows become more complex with additional steps and business logic.

This is an example of the most basic workflow. I don't have enough space to go into more depth, but if you look through the available actions for workflow steps, you'll get an idea of what's available. You can also custom-build these actions in Visual Studio and use them in SharePoint Designer. Workflows can make decisions based on user input, look up data from the current item or SharePoint lists, and span multiple users. They are capable of significant complexity.

Extremely Powerful

Although this is a quick and relatively simple display of the technology, you can see how easy it is to build custom forms with workflow, and you can get a sense of the additional power and flexibility at your fingertips. I should also point out that all the form-development functionality is similar to that of InfoPath 2007 and Microsoft Office SharePoint Server 2007. Although some of the screen layouts are different, everything we walked through can also be built in the current version of these products. Only the workflow components at the end have changed significantly in the 2010 release.

InstantDoc ID 104663

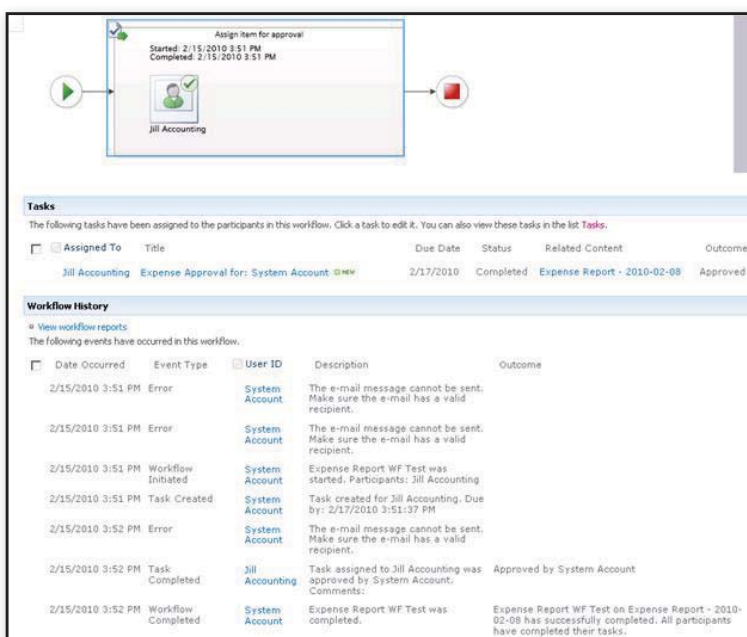


Figure 6: Approving the report



Ryan Thomas

(rthomas@syrinx.com) is director of the SharePoint Practice at Syrinx Consulting. He's a Microsoft Certified Professional Developer and Microsoft Certified Application Developer, and contributes regularly to the Syrinx SharePoint blog and other industry publications.

Going Virtual with Exchange 2010

Improvements in virtualization technology make deploying Exchange 2010 virtually a great option



Michael Noel

(michael@cco.com) is a partner at Convergent Computing, a Microsoft SharePoint MVP, and the author of books on SharePoint, ISA Server, and Exchange Server. His latest book is *Windows Server 2008 R2 Unleashed* (Sams).

Server virtualization technologies have become so commonplace that they're the de facto standard for server deployment in many organizations. It's becoming more and more common to run into data center environments that operate with the assumption that all new servers will be deployed as virtual guests—unless there's some specific reason not to virtualize. This situation is a significant change from even just a few years ago when the question was reversed, and servers were deployed on physical equipment unless there was a specific reason to virtualize.

So, what about Microsoft Exchange Server? Should you virtualize some or all of an Exchange environment and take advantage of the consolidation, optimization, and flexibility options that virtualization infrastructure provides? The reality is that Exchange environments, particularly those running Exchange Server 2010, can be robustly deployed on virtual servers as long as sufficient resources are allocated to virtual guests and the virtual hosts are scaled correctly. Deploying Exchange improperly in a virtual environment can lead to slowness and other performance problems, and can decrease management confidence in virtualization as a whole, so it's vital to review virtualization design criteria for Exchange in advance.

Microsoft's Virtualization Support Story

The support story for Microsoft products running on virtualization hardware is long and complicated. Until several years ago, Microsoft offered limited support for its flagship server products, such as Microsoft SQL Server, SharePoint, and Exchange, and left open the option that a support problem might need to be duplicated on physical hardware if support technicians couldn't determine the nature of the problem in a virtual environment. Adding to Microsoft's weak support story around the time Exchange Server 2007 was released, Microsoft's own virtualization product at the time, Virtual Server 2005 R2, wasn't a hypervisor-based product and couldn't virtualize 64-bit guests. Therefore, support for virtualization of a 64-bit-only product such as Exchange 2007 was lacking.

Two significant developments changed this story: The first was Microsoft's release of a 64-bit-capable hypervisor, Hyper-V; and the second was the development of a program called the Server

Virtualization Validation Program (SVVP), which outlined Microsoft's official support stance on running its products on third-party hypervisor virtualization platforms, such as VMware ESX Server and Citrix XenServer. This program, outlined in the Microsoft article "Support policy for Microsoft software running in non-Microsoft hardware virtualization software" (support.microsoft.com/kb/897615), allowed for support of Microsoft products on third-party virtualization products that were validated by Microsoft and complied with certain criteria, namely the ability for guest sessions to have direct access to hardware resources via a virtualization hypervisor. These two developments opened the floodgates for Microsoft servers running on virtual guests and gave peace of mind to organizations that needed to deploy supported solutions.

Exchange Virtualization Support

Exchange has been a stubborn convert for virtualization over the years. One of the main reasons for this is the fact that Exchange Mailbox servers have traditionally had high performance and disk I/O requirements, which can sometimes be a challenge to replicate on virtual hardware. Although possible to run in a virtual environment, Exchange would consume such a large portion of the resources of the host that the consolidation benefits of virtualization would be minimized. Combine this situation with Microsoft's support stance, and you can see why Exchange server has been one of the applications that has trailed many others in the number of virtualized systems in production.

Exchange Server 2003 was seldom virtualized, except for a few isolated front-end Outlook Web Access (OWA) servers or bridgehead servers. Even in those cases, Microsoft didn't support many of the configurations. Exchange 2007 was the first version to gain broad virtualization support, often at the Client Access and Hub Transport server role tiers but rarely for the Mailbox server role. Exchange 2010, however, is positioned as a great version to virtualize because of both virtualization technology advances and reduction of disk I/O requirements for the Mailbox role that Microsoft has achieved. Disk I/O in Exchange 2010 is significantly less than it is in Exchange 2007, which in itself is less than an equivalent Exchange 2003 server. As a result, many organizations are looking at virtualizing their new Exchange 2010 systems.

There are some limitations to virtualization of Exchange 2010 server roles. For example, Microsoft doesn't support virtualization of the Unified Messaging role. All other roles, however—Client Access, Hub Transport, Edge Transport, and Mailbox—are supported, provided the virtualization software is a member of the aforementioned SVVP.

In addition, Microsoft doesn't support using the Exchange 2010 native mailbox high-availability option, database availability groups (DAGs), on virtual hosts configured for host high availability. This limitation applies to technologies such as VMware's V-Motion, Citrix's XenMotion, Hyper-V Live Migration, and any other solution that automatically fails over the guest sessions from a downed host to another host server. In general, the preferred option would be to use DAG replicas, which have significant advantages, and simply deploy hosts that house the Exchange Mailbox servers without the high-availability options in the host virtualization software.

Virtualization Host Requirements

The key to a stable and high-performance virtualized Exchange environment is using the proper architecture in the virtualization hosts. Out-of-the-box settings and slow disks might work for a test environment, but Exchange has very specific requirements that need to be built into the host system for proper performance to be achieved. Therefore, be sure to follow these minimum requirements when you design the virtualization host infrastructure:

- **Allocate sufficient memory for the host OS.** If you're using Hyper-V, you'll need to reserve at least 1GB of RAM for use by the Hyper-V host. If you're using a third-party virtualization product, check with the individual provider to determine the minimum amount of memory required.
- **Allocate a dedicated NIC for management.** Each host should have a dedicated network card for host management, separate from the NIC or NICs used by the virtual guests.
- **Allocate a dedicated NIC for failover.** If you're using virtual host failover software, such as Hyper-V Live Migration, use a dedicated NIC for the failover.

Remember, however, the support limitations for using virtual host failover with Exchange DAGs.

- **Use multiple LUNs or storage arrays.** Best practice is to allocate a dedicated LUN or storage array for the host OS, another for the guest OS virtual disks, and at least one more for Exchange Mailbox server database storage.
- **Use fixed-size or pass-through VHDs.** To be a supported Exchange solution, Microsoft requires all Virtual Hard Disks (VHDs) used by Exchange servers to be either fixed-size or pass-through disks that are connected directly to a volume on the host storage. Pass-through disks give you the fastest performance, which is highly recommended for Mailbox servers. Fixed-size disks are faster than dynamically expanding disks, which can suffer performance loss when they're resizing.

The key to a stable and high-performance virtualized Exchange environment is using the proper architecture in the virtualization hosts.

- **Use a 2:1 ratio of virtual processors to physical cores.** For a virtual host to be supported for Exchange, it can't be overloaded with too many guest sessions. Microsoft caps its support levels on a single virtual host at a 2:1 virtual processor to physical core ratio. In other words, if your host is a 2-processor quad-core system (8 cores total), the maximum number of virtual processors that can be allocated and running at any one time is 16. If each guest session is allocated 4 virtual processors, for example, that caps the number of running guests at 4 on that host.

In addition to these technical specifications for the virtualization host, you'll need

to keep in mind some limitations as you set up your virtual environment. Microsoft supports Exchange servers on virtual hosts that are running only virtualization software, with exceptions made only for anti-virus and backup software. Overloading the virtual host with other software or other server roles can significantly degrade guest performance. In addition, from a Windows Server licensing perspective, running any roles other than virtualization roles on a Windows server requires one additional license. If the host runs only virtualization roles, however, the host OS isn't counted when determining the number of Windows licenses that are used as part of Microsoft's virtualization licensing program.

Don't combine the Mailbox, Hub Transport, and Client Access server roles on the same virtual guest. An Exchange server with these three roles installed on it would require more virtual processors than can be allocated to it within a single virtual guest, so although it's possible for testing, it isn't supported in production to create a virtual guest with all roles installed. Instead, use at least two virtual guests, one for the Mailbox server and the other with the Hub Transport and Client Access servers. And finally, Microsoft doesn't support reverting an Exchange server to a virtualization software snapshot or using differencing or delta disks.

As a general rule of thumb, it's always a good idea to give as much memory and as many processor cores to your virtual hosts as budget allows. Virtual hosts with multiple multicore processors and large amounts of RAM (64GB, 128GB, or more) are becoming commonplace because of the ability of the virtual host software to take advantage of the additional resources and also because host failover solutions require additional resources on each host to fail over sessions. In reality, there's a sweet spot when it comes to sizing virtualization hosts that balances the cost of the various components against the need to have fewer hosts. Generally, the virtualization overhead required to run virtual servers is only 5 percent, so the resources used by virtualization are more than made up by the advantages of using it.

Software and Licensing Notes

It's highly recommended to use the latest virtualization host software from

Table 1:	Hub Transport and Edge Transport Server Roles Resource Guidelines	
	Physical	Virtual
Maximum number of cores or virtual processors	12	4
Memory allocation	1GB per core	1GB per virtual processor
Ratio to number of Mailbox servers	1:5	1:5

your particular vendor. The latest version of Hyper-V is included with Windows Server 2008 R2. This version of Hyper-V has significant performance improvements over the original version of Hyper-V and has new features such as Core Parking, Live Migration, I/O improvements for fixed-size VHDs, TCP Offload and Jumbo Frames, and support for Second-Level Address Translation (SLAT)-enabled processors. If you're virtualizing Exchange on Hyper-V, also consider deploying the virtual host on Server Core to minimize its security footprint and memory use.

If you're managing multiple virtual host machines, centralized management software is also recommended. For example, Microsoft offers System Center Virtual Machine Manager (VMM) 2008 R2 for virtualization management. VMM 2008 allows for physical-to-virtual (P2V) server migration, server template libraries, and management of both Hyper-V and VMware hosts and guests through a single console.

Microsoft provides for cost-effective virtualization licensing options for Windows Server, which lets organizations save significantly on Windows Server licenses when virtualizing servers. The three types of virtualization server licensing are:

- Windows Server Standard Edition, which allows for a single physical OS environment (POSE) or a single virtual OS environment (VOSE) with each Standard Edition license. Note that a virtualization host that's dedicated to virtualization tasks doesn't consume a license even if it's running Windows Server (such as in the case of Hyper-V).
- Windows Server Enterprise Edition, which allows for up to four VOSEs to be run at any one time on the host. Note that only active running guests are counted against the license count, so if a guest is shut down, it doesn't count against the total.
- Windows Server Datacenter Edition, which is a per-processor license for the

virtual host (a dual quad-core server would require two licenses) that grants you the right to run an unlimited number of virtual servers on the host.

These licensing options apply not only to Microsoft Hyper-V but also to any virtual host that's a member of the SVVP. For organizations with a significant investment in virtualization infrastructure, it's most cost-effective to simply buy an appropriate number of Datacenter Edition licenses to cover all your virtual servers running across your infrastructure.

Virtualization on the Hub and on the Edge

The best virtualization candidates of the Exchange server roles are the Hub Transport and Edge Transport servers. These servers provide for message flow between mailboxes, policy control, and antispam services. They're easily virtualized and in many organizations are the first of the Exchange roles to be virtualized.

Table 1 shows resource guidelines for the Hub Transport and Edge Transport server roles. The rule of thumb is to deploy one Hub Transport server for every five

Mailbox servers and allocate 1GB of RAM for each virtual processor when the server is virtualized. These guidelines apply to Edge Transport servers as well. The typical virtual Hub Transport or Edge Transport server is allocated four virtual processors and 4GB of RAM, along with three VHDs—one for the OS, one for the transport database, and one for the transport logs. Best performance can be achieved by placing the transport database and transport logs on separate VHDs that are running on separate spindles on the host OS. If a Hub Transport or Edge Transport server with these specifications needs to handle more mail traffic, you can simply allocate additional servers with the same metrics. The size of the host OS disk should be at least 12GB plus the total amount of memory allocated to the guest, but it's good practice to size this volume larger, typically around 50GB to allow the host OS to grow in size. These recommendations go for any virtualized Exchange server role.

Client Access Server Virtualization

The next likely candidate for virtualization is the Client Access server role, which handles HTTP, HTTPS, IMAP, POP, and MAPI requests directly from clients. This role has become more important in Exchange 2010 because all client connections are proxied through the tier of Client Access servers, making them critical for access to Mailbox servers, and also increasing their resource requirements.

Table 2 shows resource guidelines for Client Access servers. Note that the RAM

Table 2:	Client Access Server Role Resource Guidelines	
	Physical	Virtual
Maximum number of cores or virtual processors	12	4
Memory allocation	2GB per core	2GB per virtual processor
Ratio to number of Mailbox servers	3:4	3:4

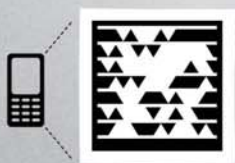
Table 3:	Combined Hub Transport/Client Access Server Role Resource Guidelines	
	Physical	Virtual
Maximum number of cores or virtual processors	12	4
Memory allocation	2GB per core	2GB per virtual processor
Ratio to number of Mailbox servers	1:1	1:1



Efficiency you can feel,
but can't touch.

Finally, a consolidated virtualized infrastructure, from the data center to the desktop, is within grasp. Well, not literally of course. After all, it's virtualized. Start with Windows Server® 2008 R2 with built-in Hyper-V™ and you can eliminate costly third-party software like VMware. Add SQL Server® 2008 Enterprise, with unlimited virtualization, and you just made it easier to eliminate racks of underutilized servers. Toss in System Center and you've centralized management across the enterprise all the way down to the application level. Translation? Flexible and dynamic virtualized infrastructures that help maximize ROI, reduce TCO and improve business continuity. Just don't let the efficiency go to your head.

To learn more about how server virtualization can make you more efficient, go to itseverybodysbusiness.com/virtual



Snap this tag to get the latest news on server virtualization or text VIRTUAL to 21710

Get the free app for your phone at <http://gettag.mobi>

Because it's everybody's  business

Table 4: Maximum Number of Mailboxes and Memory Guidelines for the Mailbox Server Role

Total Messages Sent and Received per Mailbox (75kb message size)	Mailboxes per Physical Core	Amount of RAM Above 4GB to Allocate per Mailbox (in MB)	Mailboxes per Virtual Processor
50	1000	3	900
100	900	6	810
150 (Typical)	800 (Typical)	9 (Typical)	720 (Typical)
200	700	12	630
250	600	15	540
300	500	18	450
350	400	21	360
400	300	24	270

requirements are double that of the Hub Transport and Edge Transport roles and the number of Client Access servers per Mailbox server is also much higher. Be sure to plan an adequate number of Client Access servers, virtualized or physical, for Exchange 2010. The typical virtual Client Access server role system consists of a virtual guest with four virtual processors and 8GB of RAM allocated to it. It has a single pre-sized 50GB VHD for the guest OS.

Combining the Hub Transport and Client Access Roles

It's common in many organizations to combine the Hub Transport role with the Client Access role to create a combined Hub Transport/Client Access server or set of servers. These servers can then be load balanced using either software or hardware load balancers to provide for high availability of the Client Access service.

Although combining the two roles results in additional load on an individual server session, many of the same processor and memory guidelines that apply to a Client Access server apply to a combined server, as Table 3 shows. The difference lies in the ratio of the number of Hub Transport/Client Access servers to Mailbox servers, which is increased to 1 to 1.

The typical virtual Hub Transport/Client Access server role system consists of a virtual guest with four virtual processors and 8GB of RAM allocated to it. It has a single pre-sized 50GB VHD for the guest OS and two additional pre-sized VHDs for

the Hub Transport's database and logs, respectively.

Mailbox Server Virtualization

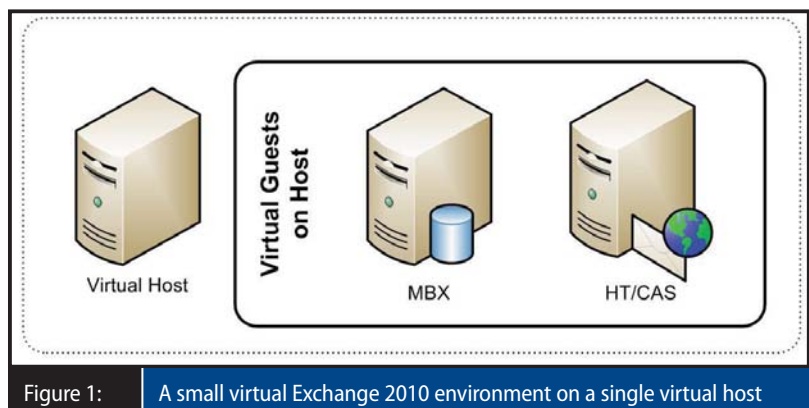
The Mailbox server is the most sensitive server role to virtualize. This is the server that needs the lion's share of RAM and processor allocation. A physical Mailbox server has the same processor limitations as the other servers do (12 cores maximum) and the same virtual limits (4 virtual processors maximum), but the memory allocation becomes more complex. The equation that's generally used when sizing the Mailbox server is to start with a minimum of 4GB of RAM, then add between 3MB and 24MB of RAM per mailbox, depending on how many messages each mailbox sends and receives daily. Using the information in Table 4, you can determine approximately how much RAM to allocate to a server and how many mailboxes can be housed on each virtual

processor allocated to the box. The average mail flow within most organizations is reflected in the table on the row labeled Typical. Your exact mail-flow statistics should be used to determine specifications for your organization.

To illustrate with an example, if you had an organization that averaged 150 75kb messages a day per mailbox and had 2,000 mailboxes, you could deploy a single Mailbox server for all the mailboxes you needed. You could run up to 720 mailboxes per virtual processor, so you would deploy four virtual processors, and you could fit up to 2,880 mailboxes on the server. Using the RAM equation, you would allocate 22GB of RAM to the server by calculating 4GB of RAM plus another 18GB (9MB × 2,000 mailboxes). Of course, you might decide to deploy more servers to provide for DAG fault tolerance or simply to provide a higher level of service, but it's important to understand what Microsoft's limitations are and not to design a system to hold more mailboxes than are listed in the table.

Most organizations don't average more than 100 or 150 75kb messages a day per mailbox; however, there are certain organizations with very high messaging requirements. These organizations should take heed of the higher memory requirements for the Mailbox role and the reduced number of mailboxes that can exist per virtual processor. For example, an organization with extremely high mail loads might consider running just over 1,000 mailboxes per virtual guest and should allocate 26GB of RAM using the earlier calculations.

Keep in mind that these guidelines are simply guidelines. Actual performance will



be dictated by the type of disk, hardware architecture, and other factors. Some organizations calculate their hardware requirements, then simply add additional RAM or reduce the number of mailboxes to be safe.

Sample Virtualized Exchange 2010 Architecture

There are many ways of deploying Exchange 2010 in virtualized environments. Some designs are more common than others, however, and reflect common needs across many organizations. For example, high availability is becoming a must for the critical messaging functionality in Exchange. All the new high-availability options in Exchange 2010 are available for virtual environments and can actually be easier to deploy because of the flexibility that virtualization provides.

Figure 1 illustrates a small virtualized Exchange 2010 environment with all components running on a single virtual host. This type of deployment doesn't have any built-in high availability or disaster recovery, but it's the simplest environment to set up and it can still take advantage of virtualization benefits and scalability. Table 5 shows sample server specifications for an environment of this size. These specifications assume 500 mailboxes on the server and an average of 150 messages sent or received per mailbox per day.

Figure 2 illustrates a typical virtualization scenario for Exchange 2010 that provides for a very high level of availability, disaster tolerance, and scalability for an environment with 2,000 mailboxes. The entire Exchange environment, including Active Directory Domain Services (AD DS) domain controllers (DCs), is deployed across three virtual hosts—two in the primary data center and one in a secondary data center. DAG replicas of all mailbox databases are replicated to all three servers, providing two backups of each database that can be automatically used in the event of a failure of the Mailbox server holding the active database. Combined Hub Transport/

Client Access servers are deployed in each location and are load-balanced in the primary site.

All of these high availability and disaster recovery options are possible without the need for shared storage, a SAN, or host

availability solutions. Table 6 lists the sample virtual host and guest architecture guidelines utilized for deployment of the solution illustrated in Figure 2.

Virtualization technologies allow for a high degree of scalability and aren't limited

Table 5: Small Virtual Exchange Environment Deployment Specifications			
Server	Memory	Processors	Disk Configuration
Virtual host	24GB RAM	2 quad-core (8 cores)	C drive: Windows Server 2008 R2 with Hyper-V; 50GB dedicated volume D drive: dedicated volume for OS VHDs E drive: 500GB dedicated volume for Exchange Mailbox and transport database and transport logs VHDs
Mailbox server	8.5GB RAM	4 virtual processors	C drive: OS, 50GB fixed-size VHD D drive: fixed-size VHD (50GB) dedicated for logs E drive: fixed-size VHD (450GB) dedicated for mailbox data
Hub Transport/Client Access server	8GB RAM	4 virtual processors	C drive: OS and transport logs; 50GB fixed-size VHD E drive: 50GB fixed-size VHD for transport database

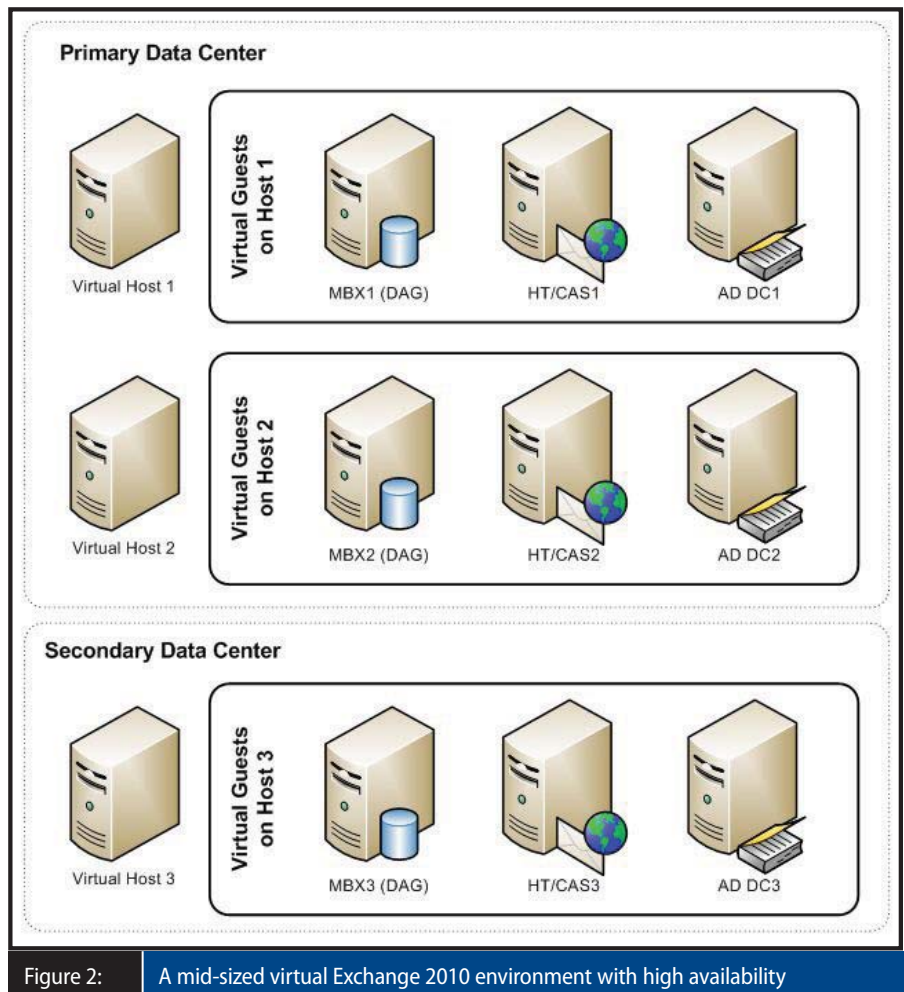


Figure 2: A mid-sized virtual Exchange 2010 environment with high availability

Table 6: Medium-Sized Virtual Exchange Environment Deployment Specifications			
Server	Memory	Processors	Disk Configuration
Virtual hosts	48GB RAM	2 quad-core (8 cores)	C drive: Windows Server 2008 R2 with Hyper-V, 50GB dedicated LUN D drive: dedicated LUN for VHDs Raw volume: 100GB dedicated LUN for Exchange log data Raw volume: 2TB dedicated LUN for Exchange mailbox data
Mailbox Servers	22GB RAM	4 virtual processors	C drive: OS, 50GB fixed-size VHD D drive: pass-through dedicated LUN (100GB) for logs E drive: pass-through dedicated LUN (2TB) for mailbox data
Hub Transport/Client Access servers	8GB RAM	4 virtual processors	C drive: OS, 50GB fixed-size VHD D drive: 50GB fixed-size VHD for transport logs E drive: 50GB fixed-size VHD for transport database
AD DS DCs	4GB RAM	2 virtual processors	C drive: OS, 100GB fixed-size VHD

to small- and medium-sized organizations. For example, the architecture that Figure 3 shows allows for tens of thousands of mailboxes, full disaster tolerance, and high availability, all with the high performance expected from Exchange. In this particular model, multiple DAG replicas of Exchange mailbox databases are spread across both virtual guests and a single physical Mailbox server for backup purposes. The server role that can't be virtualized, the Unified Messaging role, is kept on physical servers, and dedicated Hub Transport and Client Access servers are deployed as well. Finally, the management infrastructure for Exchange includes System Center Mobile Device Manager (MDM) and VMM servers integrated into the design.

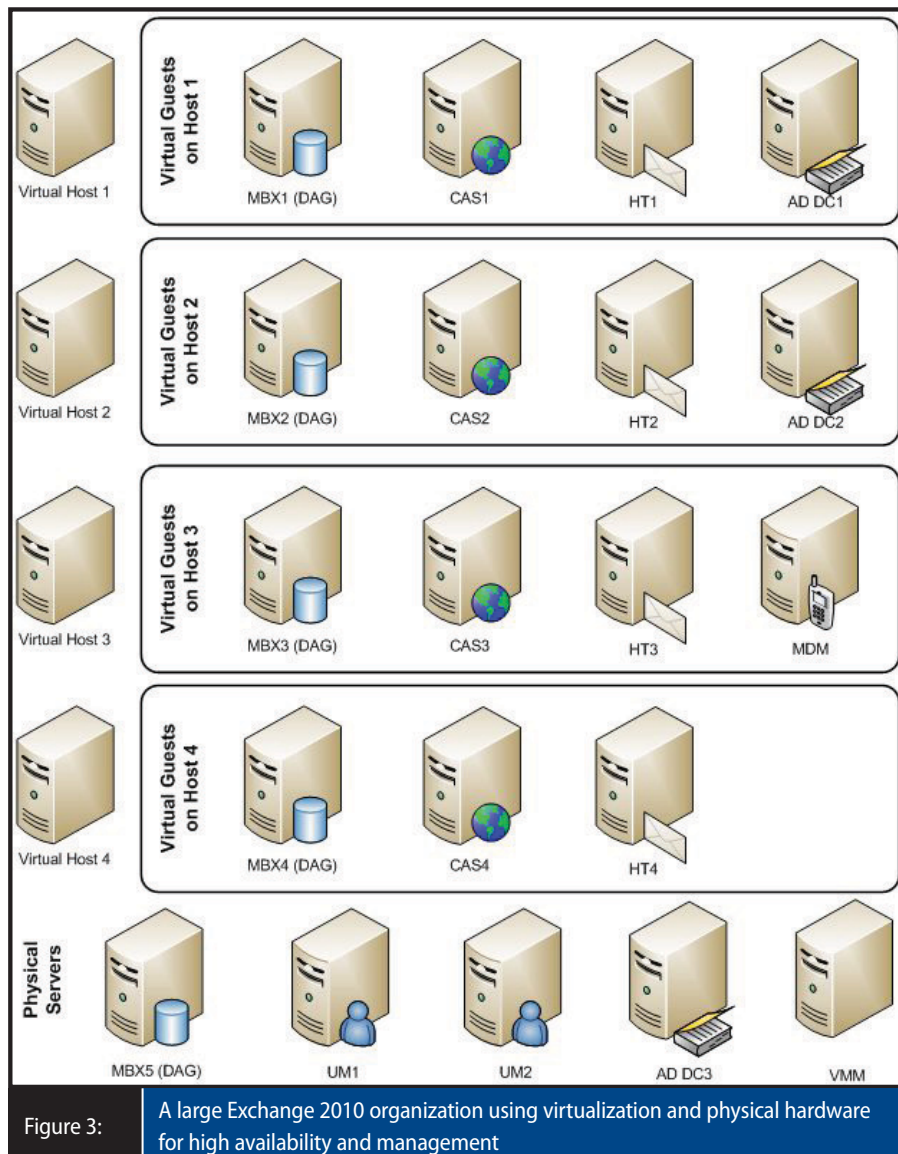
These three samples illustrate some of the potential design options that are available for a virtual Exchange environment. Every environment is unique, of course, and specifics will vary based on business and technology needs. However, you can use these sample architectures as a starting point for developing a high-performance virtualized Exchange 2010 environment.

Advantage: Virtualization

Server virtualization can provide significant advantages and can let Exchange architects design highly available and disaster-tolerant environments more easily than could be done solely on physical hardware. In addition, virtualized environments have consolidation, optimization, and cost-saving benefits that make them ideal for many organizations. With proper thought into host and guest virtualization architecture, you can deploy a fault-tolerant and high-performance Exchange environment that lets you fully capture the benefits of virtualization for your organization.



InstantDoc ID 104653



■ Network Monitoring
■ SharePoint

■ Backup and Recovery
■ Web Browsing

Anfibia Software Releases Anfibia Reactor 1.1

Anfibia Reactor is a server monitoring solution for enterprises. Features include: monitor hard drives, CPU, memory, battery life; monitor network connections such as HTTP, FTP, SMTP, POP, DNS; monitor and query databases; reboot and shut down computers; keep an error log; and restart or kill applications. Anfibia Reactor is web-based (accessible by any machine via a web browser), and installation is very simple according to the vendor. A professional license costs \$199. To learn more, visit www.anfibia-soft.com.

Panasonic ToughBook for Field Workers

Panasonic has announced the **CF-H1 Mobile Assistant**, a computing device designed for utility and field agents. It

has a rugged, ergonomic design, long battery life, and anti-reflective daylight view screen. The device is lightweight with an easy-to-grab handle, making it ideal for single-handed operation with modern applications. The ToughBook comes with wireless LAN, Bluetooth, and wireless WAN compliance. GPS is also available as an option. Mobile workers can authenticate to the device via fingerprint as well as contactless or contact smartcard readers (optional configuration). Other specs include: 10.4" display, 6 hour estimated battery life, 3.4 lbs, 1.86GHz Atom™ processor,



2GB RAM, and 64GB hard drive. Pricing and availability information were not available at time of writing.

PRODUCT SPOTLIGHT

SpectorSoft Releases New Spector Server 2010

SpectorSoft announced the release of **Spector Server 2010 - Surveillance Edition**, a new monitoring product designed for IT administrators who need to generate a detailed history, including screen recordings, of all server maintenance and session activity. Spector Server records every detail of changes being made to servers by internal IT staff, outsourced vendors, or off-site hosting personnel.

Spector Server records changes to configuration settings, modifications to startup, and batch files. It captures every keystroke typed, program run, file transferred to or from servers, and more. Administrators get a step-by-step recording of all server activity. Features include: track user log ins, detailed audit trail recording, screen recordings of specific

steps, registry and configuration change tracking, and Remote Access tracking.

"Spector Server is the first server monitoring solution to provide administrators with a visual log of activity," said SpectorSoft President C. Douglas Fowler. "As more and more companies outsource or offshore server maintenance, or use dedicated hosting providers, administrators need to keep track of everything users do. With Spector Server, they will have a record of all internal and external activity taking place on their servers."

Spector Server 2010 works on Windows Server 2008, Server 2003, Essential Business Server, Small Business Server, and Server 2000. Pricing begins at \$495. Spector Server comes with one full year of updates, upgrades, and technical support. To learn more, call 772-770-5670 or visit www.spectorsoft.com.

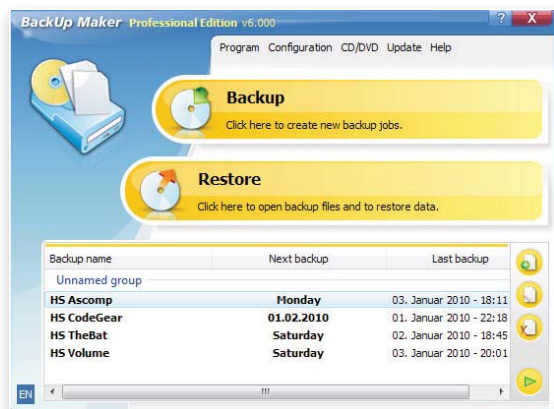
Translate the SharePoint Audit Log to English

Windows IT Pro Contributing Editor Randy Franklin Smith has released a tool called **LOGbinder SP**. According to Smith, "LOGbinder SP is a small, efficient Windows service that monitors the internal SharePoint audit log without making any changes to your SharePoint installation." From there, the program processes the data and produces an easy-to-understand translation of the audit event. Pricing starts at \$300 for Windows SharePoint Services 3.0. A free trial is available at www.logbinder.com.

BackUp Maker 6.0 Saves Time Automating Backups

ASCOMP Software GmbH has introduced **BackUp Maker 6.0**, a tool to prevent data loss and automate backups. Through the program features wizard, users can create backups triggered to events, or simply configure backup operations to be performed at specific times. The software also lets you write backup data directly to a CD or a DVD, or upload the backup to a web server. The Standard version of the program is free—BackUp Maker Professional is

NEW & IMPROVED



available for \$33.09 for an individual license and \$66.19 for a company license. To learn more, visit www.backupmaker.com.

Comodo Releases Open-Source Browser

Comodo has released **Comodo Dragon**, an open-source web browser that focuses on privacy and security. If Comodo Dragon encounters a Domain-only certificate, it warns the user that the website may not be reliable. Also, Comodo Dragon doesn't transmit information about a browsing session to a remote server, eliminating the threat that attackers could find vulnerabilities by looking for the software errors that the browser was compiling to report to a remote server. To learn more, visit www.comodo.com.

Network Monitoring in a New Perspective

ScriptLogic introduced **Perspective**, a network monitoring and management

product. Perspective centrally monitors network bandwidth, network servers, desktops, and other devices (such as routers, switches, and firewalls). Other features include: application monitoring, log file management, network traffic analysis, support for network-based services and remote offices, monitoring of virtual and cloud net-

works, and reporting and alerts. Pricing is based per monitored device. To learn more, visit www.scriptlogic.com.

Lost Data? Call in the Partition Doctor

SoftAmbulance has released a new version of **Partition Doctor**, a solution developed for recovery of your hard disk drive. Partition Doctor recovers partition tables, corrupted files, boot records, and directory structure automatically. According to the vendor, the native recovery tools in Windows are not effective enough to recover from accidental deletion, formatting errors, virus attacks, hardware crashes, and any other causes of data loss. Partition Doctor automatically scans the hard drive, and shows any recoverable files and folders. Partition Doctor costs \$139.99, or you can download a free trial at www.softambulance.com.

Paul's Picks

www.winsupersite.com



SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Office 2010 Technology Guarantee

PROS: It's a win-win situation: Buy Office 2007 now, get Office 2010 for free

CONS: Only for retail copies and PC bundles; free version of Office 2010 is download-only

RATING: ★★★★★

RECOMMENDATION: Users who purchase any version of Office 2007 between March 5, 2010 and September 30, 2010 will receive a download-only copy of the comparable Office 2010 version for free. (Those downloads must occur by October 31, 2010.) To be eligible, you must purchase Office 2007 at retail or bundled with a new PC. This is a no-brainer, and when you consider that the Home and Student version is retailing for about \$125 and can be installed on up to three different PCs, it's an even better deal for those who use Office at work and would like similar capabilities at home. There's no down side to this deal, so if you're considering Office 2010, take a look at Office 2007 today.

CONTACT: Microsoft • www.microsoft.com

DISCUSSION: tinyurl.com/office2010techguarantee

Zone Alarm DataLock

PROS: Inexpensive, provides BitLocker-like full-disk encryption for just \$20 per PC

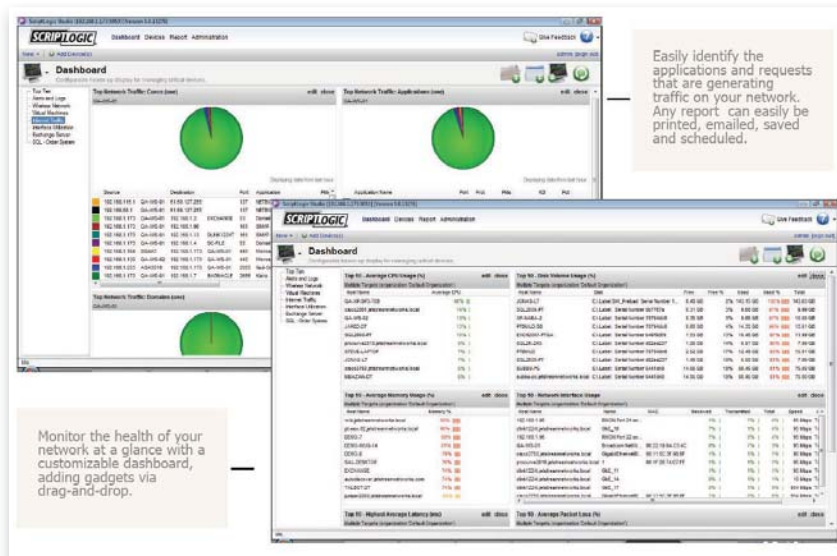
CONS: Doesn't offer functionality for USB devices

RATING: ★★★★★

RECOMMENDATION: Microsoft offers BitLocker full-disk encryption only on Windows 7 Enterprise and Ultimate, so users of the more mainstream (and affordable) Professional and Home Premium versions are out of luck. ZoneAlarm steps into the fray, however, with a low-cost solution dubbed DataLock, which offers BitLocker-like functionality without the cost. DataLock adds a second logon screen to your PC that appears at start up, and it works when offline, too, so that thieves can't attach your laptop's hard drive to another system and funnel off your valuable data. And get this: Unlike with BitLocker, there's actually a recovery process in case you ever forget your pass code. If there's a down side to DataLock, it's that it's purely consumer oriented. And of course it doesn't come with a BitLocker-To-Go-like USB device solution either.

CONTACT: ZoneAlarm (CheckPoint) • www.zonealarm.com

DISCUSSION: www.winsupersite.com/win7/home_to_pro_to_ultimate4.asp



SolarWinds ipMonitor

Network availability can be a source of much finger-pointing. Those of us running the network are usually the first to take the blame, victim to the premise that frantic calls to IT constitute network monitoring. SolarWinds joins the chorus of companies denying that premise in support of a safer ideology: early-warning systems. The company's entry-level package—**ipMonitor**—promises to provide near-instant heads-up warnings when chunks of your network hit the concrete.

The product is an agentless sentinel that monitors a network's health from afar. To do so, it use a general suite of protocols from SNMP and WMI (designed for monitoring) to basic HTTP and SQL query checks to test the core functionality of basic services.

ipMonitor's GUI is very well balanced. Accessed via the product's built-in web server, it's divided into four partitions clearly marked by function. The first of these, the Dashboard, contains a modular display of the network devices grouped by various properties. The Dashboard is the primary means by which you diagnose a problem's scope, as it aggregates warnings and alerts by type and brings them to your attention. Links to subfunctions on the other tabs are also present, enabling quick navigation of available troubleshooting resources.

The Dashboard's value becomes particularly clear when you realize it's not just a display of the worst performers on the network but rather a fully clickable menu from which you can drill your way into underlying statistics. This point-and-shoot method permits instant, fluid action rather than forcing a delay between recognizing a problem and finding the associated data.

The Devices tab, which Figure 1 shows, provides access to the network-scanning engine and its discovery process for adding new device monitors. The interface uses the term *monitor* to describe a built-in test that verifies the accessibility of a device or service. (SolarWinds offers about 50 such tests.) These tests can check ping response, successful web page loading, and Exchange Server, Active Directory (AD), SQL Server connectivity, to name a few. The benefits of the SmartMonitor feature become obvious once a scan begins, as it intelligently adds pertinent monitors to the Devices list

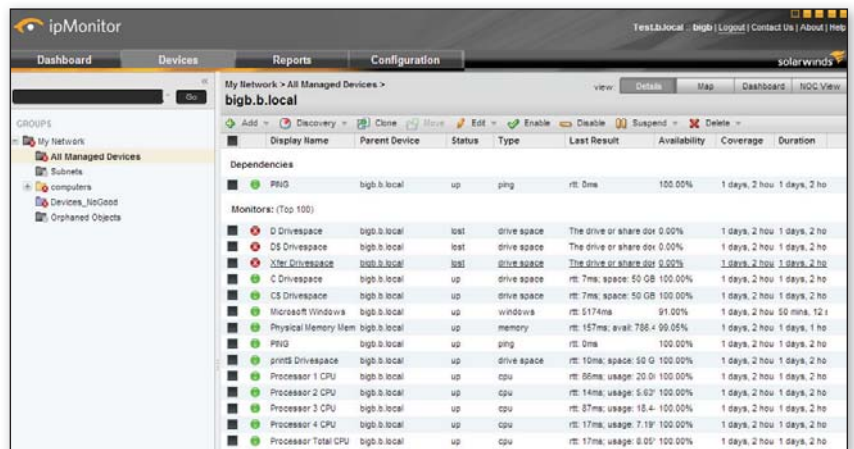


Figure 1: Using the Devices tab to access the network-scanning engine

during a sweep of the network. Because the number of monitors can be quite high, even in small networks, SmartMonitor's simplification of the process is appreciated.

An unfortunate omission from the Devices tab is the ability to sort devices by characteristic, such as status, IP address, or display name. Arguably, this kind of sorting occurs automatically on the Dashboard, but a sort option is important when working with tables that can reach significant size. The ability to create groups is helpful in this regard, but you still might ache for a way to organize this tab's data.

The Reports tab lets you quickly and easily generate reports on a per-monitor or per-group basis. The basic single-monitor reports can be queued up by device or by device group; basic reports provide quick stat-specific views, whereas custom reports can contain multiple devices in a group. Again, the tabled values here aren't sorted or sortable, which hinders data accessibility.

The Configuration tab exposes the product's less-than-obvious features, including an SNMP tree browser and search utility. Here, I must mention a crucial flaw: the relative inability to add custom SNMP Management Information Base (MIB) files to the program to enable SNMP scanning of specific devices not included with the product or on the support site. (I say "relative" because you can ask SolarWinds to add them by special

request.) You might not consider this a problem, but SNMP is well known and ubiquitous, and should be part of the basic feature set. Yes, you can add individual monitors by object identifier (OID), but that's an ancient solution for what can be easily automated.

SolarWinds' ipMonitor is a stable, low-overhead monitoring suite that serves as a watchful sentinel. (For more granular functionality, try Orion Network Performance Monitor.) Although ipMonitor fills the need for a basic yet robust tool, the lack of similarly robust, built-in custom MIB support at this price makes it a tough sell if SNMP already keeps your network humming. 

InstantDoc ID 103695

ipMonitor

PROS: Responsive, unpolished web interface; easy credential/account configuration; intuitive navigation system

CONS: Use of custom SNMP MIBs requires a support request or tedious manual process; can't sort tables of devices

RATING: 

PRICE: \$1,995 includes unlimited monitors and one year of maintenance

RECOMMENDATION: SolarWinds' ipMonitor is an excellent jack-of-all-trades monitoring program, but considering its price—which is hardly entry-level—it needs equally excellent SNMP support.

CONTACT: SolarWinds • 866-530-8100 • www.solarwinds.com



Brandon Carse | bcbigb@gmail.com

REVIEW

StarWind Enterprise HA Unlimited 5.0

Until recently, SANs were exclusively an enterprise technology. The cost and complexity of installing a SAN put it out of reach for most SMBs. Now, **StarWind 5.0** turns the storage market on its ear by providing almost all the benefits of high-end SAN storage at a price that smaller businesses can afford.

StarWind 5.0 isn't a traditional hardware-based storage device; rather, it's a software-based service that runs on Windows Server 2008 or Server 2008 R2. It requires at least a 2GHz processor, 4GB of RAM, a 1Gb Ethernet connection, and 10GB of free disk space. The StarWind Server software essentially lets the Windows Server system function as an iSCSI server. Running on Windows Server frees you from the necessity of purchasing a dedicated SAN device, and it makes the StarWind SAN extremely easy to configure and work with because you use the same Windows tool set. However, the upshot is that the base system has the same management requirements as Windows Server and requires regular patching and software updates.

I installed StarWind Enterprise HA Unlimited on a Server 2008 R2 Standard Edition system. This system had 8GB of RAM and a 2.53GHz quad-core Intel Xeon processor. The entire installation took just a couple minutes and required only 1.2MB of disk space. The product includes the StarWind iSCSI service, which permits Windows Server to act as an iSCSI target, and the StarWind Management Console, which lets you create SAN partitions out of storage attached to the Windows Server system.

Immediately following the installation, StarWind Enterprise HA Unlimited was up and running. Mysteriously, I couldn't access the StarWind Management Console either from the desktop shortcut or the Start menu but was able to open it from the system tray. Figure 1 shows the StarWind Management Console.

In the StarWind Management Console, you create iSCSI targets—essentially, storage locations. You can choose physical volumes, optical drives, or virtual disks as targets; physical disks consume the entire volume, and virtual disks are image files that StarWind creates on the physical disk. Both physical and virtual disks support clustering,

caching, and high-availability options. The product's *Getting Started* guide—including with the online Help—does a good job of stepping you through SAN setup. Oddly, you can't control the StarWind iSCSI service from the StarWind Management Console.

I tested StarWind Enterprise HA Unlimited as a Windows storage platform using basic file serving, Windows Failover Clustering, and Hyper-V Live Migration. StarWind worked flawlessly in all these scenarios. After opening firewall port 3261, I was able to use Windows Server's iSCSI Software Initiator to connect to the StarWind server with no problem and use Windows Disk Management to assign storage. The StarWind SAN passed the Windows Failover Clustering storage-compatibility test and also complied with Hyper-V Live Migration's requirements for persistent iSCSI reservations.

In my tests, the performance of the StarWind Enterprise HA Unlimited SAN was excellent. Although it might not equal the performance of a dedicated SAN, it's a fraction of the cost. It also boasts a comparable feature set. StarWind Enterprise HA Unlimited can perform storage snapshots as well as synchronous mirroring, asynchronous replication, and automatic failover between two StarWind servers.

StarWind offers a number of editions, and you need to dive into the details of each to find the feature set you want. At the low end, the basic StarWind Server—limited to 2TB of storage and four iSCSI connections—is great for testing and for R&D deployments. At the high end, StarWind Enterprise HA Unlimited has no limits on storage or connections. The license for the StarWind Enterprise HA Unlimited edition includes the right to run on two servers, letting you set up high availability at no additional cost. Check out the StarWind Editions Comparisons page

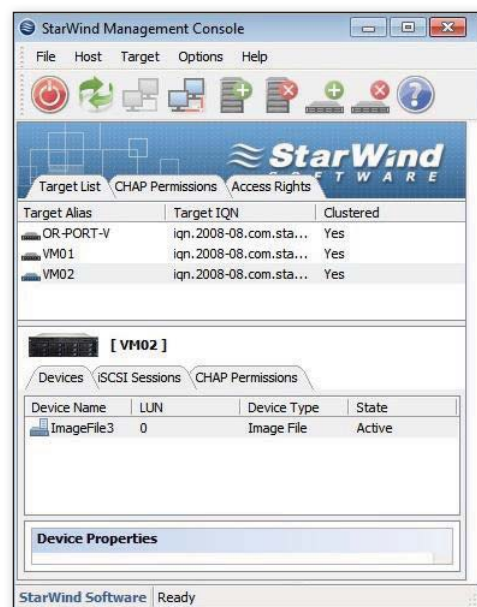


Figure 1: The StarWind Management Console

(www.starwindsoftware.com/buy/editions-comparison) for more information.

StarWind's support for VMware and Hyper-V make it a great choice for small businesses that want a SAN for virtualization or for businesses seeking an affordable iSCSI SAN for testing and development. I highly recommend giving it a close look.

InstantDoc ID 103698

StarWind Enterprise HA Unlimited 5.0

PROS: Inexpensive; easy to manage; compatible with Windows Failover Clustering, Hyper-V Live Migration, and VMware VMotion

CONS: Requires Windows Server 2008 or Server 2008 R2

RATING:

PRICE: StarWind Server \$395; StarWind Enterprise \$995; StarWind Enterprise Unlimited \$2495; StarWind Enterprise HA \$2995; StarWind Enterprise HA Unlimited \$5995

RECOMMENDATION: The StarWind SAN is a great choice for any organization looking for an affordable and easy to manage SAN solution.

CONTACT: StarWind Software • 617-449-7717 • www.starwindsoftware.com



Michael Otey | (motey@windowsitpro.com)

THE RISE OF Cloud Computing

One of the most prominent IT trends to emerge in 2009 was cloud computing. It's a technology that has been wholly embraced by vendors, but businesses remain justifiably skeptical. Even IT pundits widely disagree about the future of cloud computing: Is it yet another thinly veiled attempt to resurrect the widely rejected era of the mainframe and thin computing, or is it the basis for an all-new type of application that represents the future of computing? In these tight economic times, cloud computing's promise to cut costs makes it a compelling offering.

Let's take a look at what cloud computing can offer the average business, then see what today's cloud vendors are offering.

What Is Cloud Computing?

Cloud computing is an umbrella term for an Internet-based service that provides some type of essential service to the organization. The specific types of services vary widely. Common cloud computing services include Microsoft Exchange Server hosting, application offerings such as Google Docs, the lease of backup storage, and even relational database services such as SQL Azure. Typically, the vendor's servers entirely host these services, which you access over the Internet. However, some vendors—including Microsoft—have attempted to push a Software Plus Services model, in which locally installed software (e.g., Microsoft Office) interacts with a web-based service (e.g., Windows Live Office).

Customers typically pay the cloud computing vendor for the use of these services. Vendors usually offer some type of SLA guaranteeing specific levels of uptime and often a range of acceptable service-level performance. The types of SLAs vary with the type of service and often the level of service that the customer pays for.

The Silver Lining

Cost cutting is the primary benefit that most vendors cite for cloud computing. Cloud computing basically lets you lease essential computing services from a third party and therefore avoid the capital expenditures necessary to support these services in-house. Leasing services instead of buying and building them lets a company save in infrastructure costs, licensing costs, and the costs for the IT personnel required to run and manage those services.

Other advantages of cloud computing services are global accessibility, immediate deployment, and easy scalability. Because cloud services are Internet-based, you can access them wherever you have an Internet connection; in most cases, there are no deployment concerns. You can access the cloud-based services immediately, without any installation hassles. And cloud computing vendors have vast computing infrastructures that support very high levels of scalability. If you need additional scalability, it's often as easy as simply paying for the next level of service.

Perhaps the biggest advantages of cloud computing go to the vendors that offer the solutions. Unlike traditional software sales, cloud services use a subscription-based income model. This model lets vendors sidestep all the packaging and deployment costs typically associated with selling on-premise software. Subscription-based income is the Holy Grail for software companies because it offers a predictable income model that isn't tied to the constant release of new products.

Is it a resurgence of mainframe/thin computing, or is it the future of our business?

by Michael Otey

■ CLOUD COMPUTING

The Dark Underbelly

There's certainly merit to the notion of cloud computing, but there's also a dark side. The first concern is availability. Although the Internet and most of the involved websites are pretty reliable, the truth is that they all have downtime. When everything works, it's all transparent, but an Internet connection has many working parts, and that last mile can often be troublesome. Most cloud vendors recommend redundant Internet connections to improve availability.

However, some downtime is inevitable. The amount that's acceptable depends on the type of service. For an application such as Hotmail or backup storage, high availability isn't really a vital concern. For line-of-business (LOB) applications that your business depends on, it is. (If you're interested in using cloud services for LOB application, be sure to check the vendor's SAS 70 Audit results.) The SLAs of cloud computing vendors typically offer some amount of free services in the event of downtime.

Another concern is performance. In most cases, you're buying into an existing computing infrastructure, but you're also sharing that infrastructure with many other customers. A shared infrastructure might provide slower performance during peak usage times than you might expect. Again, for performance-sensitive services, look for SLAs that offer guarantees of acceptable performance levels.

Cloud computing also comes with potential security concerns. These solutions store your confidential data on servers that are owned by another company. Your data isn't on your premises. That might or might not be a concern. However, as Tom Casey—Microsoft's general manager for SQL Server business intelligence—pointed out in his recent interview with *SQL Server Magazine*, security hasn't been a problem with other services that most organizations are used to dealing with. For example, he pointed out that many companies have successfully outsourced payroll through Automatic Data Processing (ADP) or other providers for many years and have experienced no unacceptable security problems with sensitive data.

Another area of concern is application integration. Integrating applications that are running in boxes sitting together in the same rack can be difficult. Integrating

existing processes with external services adds another hurdle.

Finally, choosing the correct vendor for your cloud computing services is another complication. You certainly don't want your cloud computing vendor going out of business—at least not if you have critical business applications that depend on their services. Big companies such as Amazon, Google, and Microsoft aren't much of a risk, but cloud computing is an emerging

Some of the big players in the corporate cloud computing market are the usual suspects. But a few other companies that you might not expect are offering their own take on the cloud.

technology, and many smaller vendors will be vying for a piece of the cloud.

Today's Cloud Offerings

You might not realize that the first major adopters of cloud computing have been consumers. Cloud-based services such as Gmail and Hotmail have been in widespread use for years. Social-media sites such as Facebook and MySpace are also cloud-based services that millions of consumers have adopted and even take for granted.

Businesses have been more reticent to jump into the cloud. Most have already internalized important functions such as email. However, Exchange hosting is one area in which many businesses—particularly smaller SMBs that lack the expertise to manage their own Exchange servers—have been using cloud-based service for years. But cloud vendors are looking beyond Exchange, toward an entirely new type of application platform.

Some of the big players in the corporate cloud computing market are the usual suspects: Google, HP, IBM, and Microsoft all have cloud computing offerings. Other companies that you might not anticipate as cloud computing vendors, such as Amazon and VMware, also offer their own take on the cloud.

Microsoft. Microsoft's cloud-based offerings for business are primarily its new Windows Azure, SQL Azure, and Exchange and SharePoint Online services. Generally available in January 2010, Windows Azure is essentially a cloud-based version of the Windows Server OS. Likewise, SQL Azure is a cloud-based version of the SQL Server 2008 relational database server.

Unlike Windows Server, which is often used for file and print services, Windows Azure is an application platform. It runs the same types of web applications that run on Windows Server: C++, C#, and Visual Basic (VB). Pricing is structured on an as-used basis (Microsoft calls this *consumption*) or by buying longer-term contracts at fixed prices (Microsoft calls this *commitment*). Find out more about pricing at the Windows Azure Platform page (www.microsoft.com/windowsazure/pricing).

SQL Azure offers a subset of SQL Server's usual features. For example, it offers no business intelligence (BI) support and supports a restricted set of data types. Applications can access SQL Azure by using the same Tabular Data Stream (TDS) network protocol that's used to access the on-premise version of SQL Server. A SQL Azure Web edition provides 1GB of storage at a cost of \$9.99 per month, and a SQL Azure Business edition provides up to 10GB of storage at a cost of \$99.99 per month. For more information about SQL Azure, refer to "Getting Started with SQL Azure Database" (Instant-Doc ID 103133).

It's a mystery why Exchange and SharePoint Online don't fall under the Azure umbrella. Perhaps it's because they run on traditional hosted Windows Server systems rather than on Windows Azure. In any event, both products are essentially Microsoft-hosted servers. In each case, Microsoft offers a standard version (which runs on shared hardware) and a dedicated version (in which the hosted servers are dedicated solely to your company).

Microsoft also offers a Business Productivity Online Standard Suite, which includes Exchange Online, SharePoint Online, Office Live Meeting, and Office Communications Online. Find out more about this suite at Microsoft's "Business Productivity Online Standard Suite" page (www.microsoft.com/online/business-productivity.mspx). Microsoft sells a bewildering array of individual online services that you can find on the "How to Buy" page (www.microsoft.com/online/buy.mspx).

Google. Google got its start in the cloud, so it's no surprise that it's an established player in this arena. Google offers Google Docs, Google Apps, and Google App Engine cloud-based services.

Google Docs is a free service that lets you create, share, and collaborate on documents, spreadsheets, and presentations. You access Google Docs through a web browser; it requires zero footprint, and it's ready to be used right away. Some small businesses use Google Docs as an alternative to Office. Although not nearly as full-featured as Office, Google Docs provides essential word-processing and spreadsheet capabilities. Google Docs lets you import most Office document formats, including .doc, .docx, .xls, and .xlsx. Recent enhancements also enable offline document editing. Find out more at the Google Docs page (www.google.com/docs).

Google Apps is collection of web-based services, including Gmail for business, Google Docs, Google Calendar, Google Groups, Google Sites, and Google Video. Of course, Gmail provides email services, and Google Calendar provides an Outlook-like calendar with appointments. Google Groups helps you set up a documents calendar and site sharing for groups of users. Google Sites lets you create and host websites, and Google Video lets you post, play, and search for online videos. Google promotes Google Apps as an alternative to hosted email solutions such as Exchange and Lotus Domino. Google Apps costs \$50 per year, per user. There are several Google Apps editions, including Standard, Premier, Educators, Non-Profit, and Government. The City of Los Angeles is probably the highest-profile customer for Google Apps. Find out more at the Google Apps page (www.google.com/a).

Google also provides a service called Google App Engine, which lets you run your web applications on Google's servers.

Google App Engine supports Java and Python applications. Find out more at the

Google got its start in the cloud, so it's certainly no surprise that the company is now an established player in the cloud-computing arena.

Google App Engine page (code.google.com/appengine). And Google provides a free public DNS service at 8.8.8.8.

IBM. Not to be left out of the cloud race, IBM provides a number of cloud-based services. The company's LotusLive iNotes service offers cloud-based email. LotusLive iNotes supports both Outlook and Lotus Notes clients and can be accessed using POP3 or IMAP protocols. IBM provides hosting and anti-spam and antivirus protection. The company offers a free 30-day trial, as well as a mail-only service for \$3 per month, per user (or a \$3.75-per-month version that includes mail and calendar-ing). Learn more on the LotusLive iNotes page (www.lotuslive.com/en/services/inotes).

You expect to see Google, HP, IBM, and Microsoft in the enterprise cloud computing market, but you might not expect to see Amazon.

For file sharing, messaging, and collaboration, the company offers IBM LotusLive,

a collection of services that includes Lotus Meetings, Events, Connection, Engage, and Notes. These services provide a variety of business functions, such as instant messaging (IM), desktop and application sharing, slide presentations, video sharing, dashboards, and file sharing. The services are priced separately, ranging from \$79 per month to \$9 per month. Learn more about the product or try a 30-day free trial at the LotusLive page (www.lotuslive.com/en/compare).

For enterprise BI, IBM offers IBM Smart Analytics Cloud, which is essentially a private cloud consisting of IBM's Cognos BI Analytics software running on a System z mainframe. The goal of this offering is to provide BI as a service to the enterprise. Find out more at "Smart Analytics Cloud for System z" (www-03.ibm.com/systems/z/solutions/cloud/smart.html).

IBM also offers online storage with its IBM Smart Business Storage Cloud service, a highly scalable virtual-storage solution that lets you quickly provision storage for your enterprise on a global basis. Find out more at the "Smart Business Storage Cloud" page (www-935.ibm.com/services/us/index.wss/offering/its/a1031610).

IBM offers a couple cloud-based services as a service to developers: IBM Smart Business Test and IBM Smart Business Development and Test. With Smart Business Test, IBM will set up and configure physical and virtual resources—including OSs, middleware, and storage—for your company to use in testing products and services. Find out more on the "Infrastructure Optimization Services—IBM Smart Business Test Cloud" page (www-935.ibm.com/services/us/index.wss/offering/middleware/a1030965). There's also a new IBM Smart Business Development and Test program that's in beta at the time of this writing. This offering links shared cloud storage and development capabilities with IBM's Rational line of development tools.

HP. Aimed at SMB customers, HP's Communications as a Service program provides interactive voice response, video surveillance, IP contact centers, and unified communications (UC) services. The interactive voice response and IP Contact Center are customer-service-oriented solutions that let SMBs provide customers with telephone transaction services and call response services. The video surveillance solution combines on-premise

■ CLOUD COMPUTING

camera with cloud-based management and alerting services. The UC service provides a combined interface for voice, IM, and video calls using a PC or phone. Learn more at the *HP Communications as a Service* program page (h20208.www2.hp.com/cms/solutions/rc/caas.jsp).

HP also offers its Cloud Consulting Services and Cloud Assure service, consulting services designed to help you design, manage, and secure your cloud computing solutions. Learn more at the HP Cloud Consulting Services page (https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-23^41773_4000_100) and the Cloud Assure page (https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11%5e40898_4000_100__).

Amazon. You expect to see Google, HP, IBM, and Microsoft in the enterprise cloud computing market, but you might not expect to see Amazon. Well known for its web storefront, Amazon also offers its Amazon Elastic Compute Cloud (EC2) web service, along with its Amazon Simple Storage Service (S3), Amazon SimpleDB, Amazon Relational Database Service (RDS), and Amazon Simple Queue Service (SQS).

Amazon EC2 is a virtual computing platform that lets you buy multiple server instances with different levels of compute power and different OSs, including Windows Server 2008 or 2003, as well as Red Hat Enterprise Linux, openSUSE, and others. Amazon EC2 prices range from \$.95 per hour to \$3.16 per hour, depending on the level of service and the options chosen. You can also elect to reserve services on one-year or three-year terms. Find out more at the Amazon Elastic Compute Cloud (Amazon EC2) page (aws.amazon.com/ec2). In conjunction with EC2, Amazon offers a storage service called Amazon Elastic Block Store (EBS), which provides block-level storage for EC2 instances. Customers are charged by the amount of storage used at a rate of \$.10 per GB, per month. Find more at the Amazon Elastic Block Store (EBS) page (aws.amazon.com/ebs).

Amazon S3 is a web service that you can use to store and retrieve data. Stored objects can range from 1 byte to 5GBs. There's no limit to the number of objects that you can

store. Data is stored and priced according to the your region. Amazon provides two US regions and 1 European Union (EU) region. Amazon S3 is priced according to the region and the level of storage. Tiers range from 50TB to 5,000TB. Find out more at the Amazon Simple Storage Service (Amazon S3) page (aws.amazon.com/s3).

Whereas S3 is simple object-based storage, Amazon also offers two more capable storage engines: Amazon SimpleDB and Amazon Relational Database Service (RDS). Both are suitable for application development. Amazon SimpleDB provides

Cloud computing provides an Internet-based platform that lays the foundation for a new generation of globally accessed, highly scalable cloud-based applications.

high availability and automatic indexing and performance tuning. You can get started with Amazon SimpleDB for free; after that, Amazon charges \$.14 per machine hour consumed. There's also a charge on consumed data, which starts at \$.15 per gigabyte for the first 10GB and scales to \$.08 per gigabyte with 150TB of data consumed. Amazon RDS is a web service that gives you more control over the relational database. It essentially gives you access to a hosted MySQL 5.1 database. Amazon charges for Amazon RDS according to computing calls, beginning at \$.11 for 1.7GB of memory and one virtual core. Find more at the Amazon SimpleDB and Amazon Relational Database Service (Amazon RDS) pages (aws.amazon.com/simpledb and aws.amazon.com/rds).

VMware. Another company that you might not expect to see in the cloud computing space is VMware. This company's

main thrust is in using its virtualization technology to build a private cloud with its vSphere virtualization platform. The company's VMware Cloud OS and vCloud Express offerings also extend VMware's virtualization platform to the cloud.

VMware isn't a service provider; rather, its goal is to provide technologies that let partners build cloud-based infrastructure offerings. VMware Cloud OS aims to deliver a cloud-based OS through a combination of Application Services and Infrastructure Services. VMware defines a cloud OS as managing a large collection of infrastructure resources rather than managing a single server resource such as a traditional OS. Learn more at the VMware Cloud OS page (www.vmware.com/products/cloud-os/index.html).

Unlike most of the other cloud computing solutions that offer software as a service, vCloud Express offers Infrastructure as a Service (IaaS). VMware's vCloud Express will be made available through partners. Learn more at the VMware vCloud Express page (www.vmware.com/appliances/services/vcloud-express.html). Discover featured partners at the VMware Featured vCloud Service Providers page (www.vmware.com/partners/alliance/service_provider).

Where the Winds May Blow

Unlike the failed thin computing trend a decade ago, cloud computing is here to stay. As you can see, a wide variety of companies offer solutions that range from user-oriented solutions to enterprise development platforms. At this point, cloud computing might not be for all businesses—and it isn't going to replace on-premise solutions anytime soon. However, it's a way to extend the capabilities of your organization with a minimum of capital expenditures. In addition, cloud computing provides an Internet-based platform that lays the foundation for a new generation of globally accessed, highly scalable cloud-based applications. 

InstantDoc ID 103674



Michael Otey

(motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

Group Policy Management Tools

Manage and control change in the complicated world of GPOs

by Caroline Marwitz

Group Policy began in Windows 2000 with just 500 settings. Windows XP SP2 had 800 additional settings. With Windows Vista, you'll find 3,000. And Windows Server 2008 added over 3100 policy settings in administrative templates and over 175 security policy settings. Group Policy secures and regulates the essentials your organization needs to run smoothly, from critical business applications and processes to settings on users' computers and printers. But try to manage Group Policy and soon enough, even your above-average knowledge can get you in trouble.

The alternative is to avoid touching Group Policy or mess with it as little as possible. In fact, many admins admit that their "strategy" for determining whether they've successfully configured Group Policy properly is to wait for an incident to occur. Then the problems begin.

At the least, your fellow admins and staff have to drop other projects to work on untangling Group Policy knots. At worst, a Group Policy mistake might go undiscovered, or a disgruntled or incompetent admin could alter policy settings, weakening security or potentially causing a data breach.

Microsoft to the Rescue—Not

When Microsoft brought out the Group Policy Management Console (GPMC), it was a welcome addition to Group Policy. Granted, it has helped admins manage Group Policy better, particularly in organizations where not many Group Policy changes are typically made. But where there are frequent changes and multiple administrators involved, the GPMC isn't satisfactory in monitoring and controlling Group Policy changes.

Then Microsoft proffered Advanced Group Policy Management (AGPM), acquired as part of Desktop Standard's technology. AGPM offers admins the ability to check in and check out GPOs while editing them, and it lets admins compare two GPO versions and roll back to a previous GPO version. Another nice touch is the ability to create GPOs from templates and to delegate access to GPOs. The catch is that you have to be a Windows Software Assurance (SA) customer, as it's part of the Microsoft Desktop Optimization Pack (MDOP), which is only available to SA customers.

Filling in the Gaps

Third-party solution providers have tackled the Group Policy management gaps in their own ways. They offer a wide range of solutions, from tools that automate Group Policy management tasks,

to tools that monitor and audit Group Policy changes, to tools that extend Group Policy and help you lockdown desktops using least privilege, to tools that let you combine various aspects of the above. You can find Group Policy management tools that delegate access, allow check-in and check-out, and offer version control. In addition, many also offer offline repositories of GPOs where you can edit and try out policy settings in the comfort of a test environment rather than putting them directly into a production environment. Many of these tools extend the GPMC to help you create GPO changes, then verify and compare versions of your GPOS to maintain consistency. Some help you make your desktop and application configuration more uniform and increase their security. Some alert you to changes in GPOs. Some let you create or use policy settings that aren't even part of Group Policy, to assist in becoming compliant with your auditors and with specific regulatory requirements.

In this Buyer's Guide, we depart from our traditional format somewhat to better offer you a look at a variety of Group Policy management tools. (See Table 1 for product information.) We've rather broadly interpreted management: Some of these tools help you manage Group Policy by automating tasks; others help you by tracking GPO changes; still others help you by extending what Group Policy can do. As prices change depending on licensing and numbers of machines, we leave it to your initiative to get price quotes.

Additionally, we like Group Policy tools that extend Group Policy, making it do what it should have been able to do by itself by now. If you already have a Group Policy management tool and would like to get even more out of Group Policy, look into these solutions as well:

- Avecto Privilege Guard (www.avecto.com)
- BeyondTrust Privilege Manager (www.beyondtrust.com)
- FullArmor Policy Portal (www.fullarmor.com)
- PolicyPak Software PolicyPak Professional with PolicyPak Design Studio (www.policypak.com)
- Special Operations Software Specops Command and Specops Deploy (www.specopssoft.com)



InstantDoc ID 103691



Caroline Marwitz (cmarwitz@windowsitpro.com) is an editor for *Windows IT Pro*, *SharePointPro Connections*, and *SQL Server Magazine*, specializing in Active Directory, Group Policy, and SharePoint.

Company	Product	Uses Microsoft Group Policy Management Console (GPMC)	Offline GPO Repository	Change Management	Change History	Enforces Policy Offline	Version Control	Rollback
Blue Lance www.bluelance.com 800-856-2583	LT Auditor+ 9 for Group Policy, part of LT Auditor for Windows			Yes	Yes			
NetIQ www.netiq.com 888-323-6768	Change Guardian for Group Policy			Yes	Yes			
	Group Policy Administrator		Yes				Yes	Yes
NetWrix www.netwrix.com 888-638-9749	Group Policy Change Reporter	Yes		Yes				
New Boundary Technologies www.newboundary.com 800-747-4487	Policy Commander			Yes		Yes		
Quest Software www.quest.com 800-306-9329	GPOAdmin	Yes	Yes	Yes			Yes	Yes
	Quest ChangeAuditor for Active Directory			Yes				
SDM Software www.sdmsoftware.com 415-670-9302	GPEXpert Group Policy Automation Engine			Yes				
	GPEXpert Backup Manager for Group Policy	Yes					Yes	Yes
SysPro www.sysprosoft.com	PolMan			Yes				

Editor's Note: Information in this buyer's guide comes from vendor representatives and resources and is meant to jump-start, not replace, your own research; also, it is not necessarily comprehensive, as some products might have been left out due to the writer's oversight.

	GPO Backup	Scheduled Backups	Compares GPOs	Auditing	SQL Server Express or SQL Server	Alerting	Reporting	OSs Supported
				Yes	Microsoft SQL Server 2005 or SQL Server 2000		Yes	Windows Server 2008, Windows 7, Windows Vista, Windows Server 2003, Windows XP, Windows 2000 Server SP4
				Yes	SQL Server 2000 SP3	Yes	Yes	Server 2008, Vista, Windows 2003, XP, Win2K
					SQL Server 2008 Standard or Enterprise Edition or SQL Server 2005 Standard or Enterprise Edition SP2		Yes	Server 2008, Vista SP1 or 2, Windows 2003 R2 SP2, XP SP3
	Yes	Yes	Yes	Yes	SQL Server 2008 or 2005 with Reporting Services (SSRS) or SQL Server Express Edition with Advanced Services		Yes	Server 2008, Windows 2003, Win2K
				Yes	SQL Server 2005 or SQL Server 2000 SP3	Yes	Yes	Vista, Windows 2003, XP, Win2K
	Yes	Yes	Yes	Yes		Yes	Yes	Windows 7, Vista, Server 2008 R2, Server 2008, Windows 2003 R2, Windows 2003, XP SP2
				Yes	SQL Server 2008 or SQL Server 2008 Express Edition with Advanced Services or SQL Server 2005 (RTM, SP1, or SP2)	Yes	Yes	Server 2008, Vista, Windows 2003, XP SP2, Win2K Pro SP3, Win2K SP3
				Yes				Server 2008 R2, Server 2008, Windows 7, Vista, Windows 2003, XP
	Yes	Yes	Yes					Server 2008, Vista, Windows 2003, XP
			Yes	Yes			Yes	Win2K and later

One image
Any device
No 0x000000007B

**DOWNLOAD A FREE
30-DAY TRIAL**

The only deployment
solution with driver
packages included

Save thousands with
per-technician licensing

No need to modify
images for different
hardware

No need for dedicated
hardware

No connected services
required

Manage your entire
business with a single
toolset

OFFER EXTENDED!
WINDOWS IT PRO
SUBSCRIBERS
RECEIVE 20% OFF
THROUGH JUNE 2010



■ Security Wishlist

■ Motorola Droid

INSIGHTS FROM THE INDUSTRY

IT Security Wish List for the 2010s

Well, new website, new year, new decade. I figure I should look forward rather than backwards, so if the IT gods are listening, I have a wish list for the InfoSec industry this decade.

1. IDS/IPS that actually works. Intrusion detection/prevention systems have perpetually been a day late and a dollar short. At best, even when systems are monitored faithfully 24/7 by trained experts, you are reacting to an incident that has either already happened or is in progress. I'd like to see IDS systems that are predictive rather than reactive. Cisco's IPS version 7.0, armed with a central Cisco-run repository that keeps track of all the bad actors so that you don't have to, is a step in the right direction. We need to centralize recording and analyzing incidents and alerts like we've done with spam and viruses to companies that are better suited to handle this job.

2. Ending the spam/anti-spam arms race. It seems like we beat back the spammers for a few months and then they come out with a new trick or algorithm and our mail boxes overflow again until the vendors catch up. The only real way out of this vicious circle is a true whitelist technology, probably also coordinated by a central resource. Unfortunately, the most likely vendor for this is Microsoft—not everyone's favorite for controlling such an important resource. However, they've made some inroads in that direction and building into Windows would instantly cover a large portion of email users. Someone will need to find a system where it is easy to register your email as valid, hard to fool, and gets a high subscription rate.

3. A happy medium for responsible disclosure of security holes. The current battle between companies and security researchers makes no one happy. If the researcher tries to work with the company, they are branded as not independent and catering to the vendor over the interests of users. If they release the information

without waiting for the vendor to patch, then they are excoriated as irresponsible and helping the hackers. Both sides are guilty of not playing nice with each other. Perhaps what we need is a disinterested party to manage this. Maybe some rich retired techie will fund a foundation to process security disclosures, notify the companies, and give a fair amount of time to fix the problems before public disclosure.

4. Patching software becomes a thing of the past. I don't mean that we just stop patching. I mean that the need to patch software goes away. When you think about the fact that broken software requires you go out and research, download, install, and troubleshoot new software to fix the old software, you realize that it's a system doomed to failure. In the future, I'd like to see software smart enough to phone home once in a while, check for any fixes, and automatically fix itself without any user invention.

5. Single Sign On (SSO) becomes a reality. Who isn't tired of remembering dozens of ever lengthening passwords for all your systems? No one, but it's currently the only way to keep up with the ever more powerful password crackers and brute force tools. It's a similar conundrum to the spam issue, unless we finally figure out a sane way to do SSO using strong, hardware-based crypto. We've figured out how to do it for physical IDs (e.g., state driver's licenses issued by the state). It is an entity well suited to verify our identity and with the resources to manage the process and prosecute fraud. We've even figured it out for web-based encryption (SSL certificates) and that uses private, distributed authorities to manage the credentials.

6. Microsoft. Do something. Insert your own wish for the software behemoth here. And die isn't an option.

7. Credit card companies and merchants get serious about security. It

would be nice if they would finally take the security of our identities as seriously as we take it. Penalties need to be harsher: perhaps a public version of the stockade, where companies that abuse our trust and lose our identities are publicly humiliated. And would it be too much to ask them to make the application process for credit harder to limit ID thieves from going into BestBuy with my ID, filling out an application that is shorter than the McDonalds job application, and letting them walk out with a truck full of new electronics on my bill?

8. Companies get serious about IT security. It seems like unless the government or some regulatory body holds a gun to their head, most companies still treat IT security as a red-headed step child. They often see it as something that doesn't put money on the bottom line and is a zero sum game. The only industries that actually spend serious time and effort on IT security are the ones that are regulated by Uncle Sam (or Uncle State or Uncle Local).

9. Treat security as a National Security threat. Speaking of government, maybe our government will finally get its head out of a well-known place and figure out that IT security is as integral to National Security as A-bombs, tanks, and full-body scanners. Come to think of it, all those things depend heavily on IT security including the design plans, operational systems, and physical security systems.

10. A Black Ops commando team who will just kill all online fraudsters and save us all the trouble. OK, maybe I'm taking my flight of fancy too far. But, maybe the hackers, crackers, and online criminals would just agree to not get smarter, not get bigger and more well financed, and not get more vicious and determined to rob us all blind. I guess that's wishful thinking too.

—Tony Howlett

Choosing a Smartphone: My Choice

I've been hunting for a smartphone for several weeks now and asking for feedback from all of you about what to choose. I wanted my choice to be something Exchange administrators are currently having to support, as well as being something that is likely to be an enterprise standard device in the years to come. Many readers took part in the polls I posted to get feedback on the best features, mobile OS, and hardware vendors. Now it's time to reveal my choice.

Drum roll, please: I'll be using the Motorola Droid.

OK, it's not that dramatic. But I'm very happy and excited about my choice, and I look forward to getting to know the device when it arrives. In the meantime, I'd like to go through some of my decision process.

To start with, I felt inclined to choose a Windows Mobile device. As we're *Windows IT Pro*, using a smartphone based on Windows just seemed appropriate, even with the knowledge that Microsoft's mobile OS currently trails well behind other mobile OSs in features and functionality. The results from the polls I included with my first post on this topic (InstantDoc ID 103473) actually seemed to indicate that Windows Mobile is still more prevalent out there now than I'd thought, and Windows Mobile 6.5 is a promising update.

When I asked, in my second post (InstantDoc ID 103505) about which mobile device makers were most reliable, HTC was the runaway leader, with Motorola a distant second. Because my IT department would be supplying my phone—and related contract—I knew I was looking for a phone on the Verizon network. However, HTC's choice for running on WinMo 6.5 with Verizon is limited to the HTC Imagio, which is apparently not using the most up-to-date processor; many reviewers complained that the Imagio runs slow and freezes up when running multiple apps.

And now, of course, Microsoft has begun discussing their next mobile platform permutation, dubbed Windows Phone 7 Series. It looks fairly impressive. It has a chance to win back some market share for Microsoft. But it's still months away from availability—

and no existing devices will be able to upgrade: It's a new beast, requiring new hardware. And in any case, I can't really wait till Christmas to make a choice.

Meanwhile, throughout my search, I kept receiving nudges toward the Android OS and the Droid in particular. One of the first steps I took on my search was to see what our Exchange expert, Paul Robichaux, thought of the current crop of mobile OSs. His take on Android was that it's a "wildcard" with a shot at establishing a real presence in the enterprise market—possibly at the expense of RIM BlackBerry and other front-running mobile platforms.

Many people believe that a single mobile platform won't dominate the market in the foreseeable future. And when I asked in a poll what readers thought likely, most seemed to agree with this point.

Then last week, I spoke to Brian Reed, chief marketing officer of Box-Tone, makers of mobile device management and monitoring solutions. In talking with him about BoxTone's predictions for mobile management by 2015, he also pointed to Android as one of the three mobile OSs likely to continue to thrive, along with iPhone and BlackBerry devices. Reed felt that Microsoft has a chance to crack the top three with its Windows Phone 7 Series, but it's too early to tell for certain.

As I pointed out when I asked about which specific features were necessary for a business-class smartphone, I'm a little leery of using a touch screen, but most readers seem to believe touch screens increase productivity. I'm willing to give it a shot. But when it came down

to it, I really like the physical keyboard option on the Motorola Droid; that was probably the biggest factor in my choice of this particular device. But even the Droid's on-screen keyboard seemed more accurate than the other touch screen models I sampled at my local Verizon store. And with my clumsiness with touch screens so far, the fact that the Droid isn't multitouch actually shows up in the plus column for me.

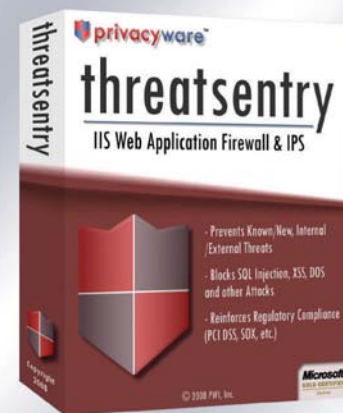
I guess I'd say that along with everything else, the cool factor of the Droid was an influence in my choice as well. It's such a sleek and beautiful-looking device, with a big, hi-res screen.

There's much more to talk about, I'm sure, but I'll save it for future posts. And naturally I'll keep you informed of what I think of the Droid and the smartphone experience in general as I get further into it.

—B. K. Winstead

Are Your IIS Servers Under Attack?

Block all unwanted IIS traffic with ThreatSentry



threatsentry
IIS Web Application Firewall & IPS

- Prevents Known, New, Internal/External Threats
- Blocks SQL Injection, XSS, DOS and other Attacks
- Reinforces Regulatory Compliance (PCI DSS, SOX, etc.)

download free trial

- IIS web application firewall & IPS
- stops known, new and internal threats
- blocks sql injection, xss, dos and more
- reinforces regulatory compliance

Microsoft GOLD CERTIFIED Partner | IIS/Software Solutions Data Management Solutions

sales@privacyware.com • www.privacyware.com • 732.212.8110 x235

For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.

COMPANY/URL	PAGE	COMPANY/URL	PAGE	COMPANY/URL	PAGE
Diskeeper Corporation	5	Microsoft	3	Privacyware	78
www.diskeeper.com		www.itseverybodysbusiness.com/deploy		www.privacyware.com	
GFI	Cover Tip, C2, 1	Microsoft	12, 13	Prowess Corporation	76
www.gfi.com/wwb		www.microsoft.com		www.prowess.com	
HOB	Cover 3	Microsoft	58-64	SharePointPro Connections	50
www.hobsoft.com/DoD2		www.itseverybodysbusiness.com/virtual		www.sharepointproconnections/subscribe.aspx	
IBM Corporation	29	Netikus	16	Sunbelt Software Inc.	Cover 4
www.ibm.com/hs22		www.eventsentry.com/AAM5		www.TestDriveVipre.com	
IBM Corporation	31	Netwrix Corporation	14	Windows IT Pro	53
www.ibm.com/systems/3monthroi		www.netwrix.com		www.windowssitpro.com	

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

Amazon	72	Motorola	78	SoftAmbulance	66
Anfibia Software	65	NetIQ	74	SolarWinds	67
ASCOMP Software GmbH	65	Netwrix	74	SpectorSoft	65
Blue Lance	74	New Boundary Technologies	74	StarWind	68
Comodo	66	Panasonic	65	SysPro	74
Google	71	Quest Software	74	VMware	72
HP	71	ScriptLogic	66	ZoneAlarm	66
IBM	71	SDM Software	74		

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowssitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.

www.windowssitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.

www.wininformant.com

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

asp.netNOW

Exchange & Outlook UPDATE

SharepointPro Connections UPDATE

Security UPDATE

SQL Server Magazine UPDATE

DevConnections UPDATE

Windows IT Pro UPDATE

Windows Tips & Tricks UPDATE

WinInfo Daily UPDATE

www.windowssitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

Super CD/MP

Get exclusive access to all of our print publications, including *Windows IT Pro*, via the new, banner-free VIP Web site.

www.windowssitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.

www.windowssitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.

www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.

www.devproconnections.com

Office & SharePoint Pro

Dive into Microsoft Office and SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.

www.officesharepointpro.com

NEW WAYS TO REACH

WINDOWS IT PRO EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: <http://tinyurl.com/d5bquf>. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowssitpro.

Windows IT Pro

Gadgets!

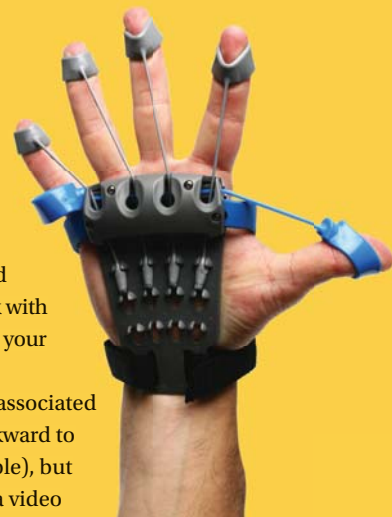
The Xtensor Tackles Sore Wrists

by Brian Reinholz

The Xtensor is a glove-like tool that claims to strengthen muscles in the hand, forearm, and elbow to cure ailments (e.g., tendinitis, carpal tunnel syndrome) caused by repetitive work with the hands, such as typing at a keyboard. The science is simple: Using the Xtensor stretches your fingers against resistance, counterbalancing the negative effects of constant typing.

In my testing, I found that, yes, the Xtensor does reduce much of the stress and pain associated with plunking away at a keyboard or BlackBerry for hours on end. The device is a bit awkward to fit your hand into (surely you didn't expect something called an Xtensor to be comfortable), but you'll really feel a healthy burn after only a minute or two of use. (The Xtensor includes a video demonstration illustrating correct use.)

A potential pitfall is that the Xtensor is a one-size-fits-all device, so if you have very small or very large hands, you might have a problem. It does come with a number of different finger bands at various sizes, so you can pick the sizes that work best for you. I would add that the \$39.95 price tag seems a bit steep, but if you're dealing with recurring wrist pain, the Xtensor might be a bargain, considering the cost of other therapies. You can purchase the Xtensor at www.thextensor.com.



The Modus 1 Illuminates the Server Closet

by Jason Bovberg

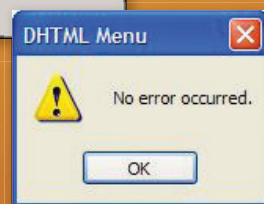
The Icon Modus 1 is a tough, nimble, aesthetically cool little flashlight that's perfect for the IT guy poking around a dimly lit server room. This white polymer beauty fits perfectly in the hand, giving you easy thumb-control of power and brightness. Powered by a single AA battery, the Modus 1 puts out modest power, but it really makes the most of its illumination with its double-LED optics system.

What I like most about the Modus 1 is its generously wide output, particularly when contrasted with the focused beam of a traditional flashlight. I used the Modus 1 in the very scenario an IT pro might use it: cabling a computer in a darkened area. The flashlight proved indispensable, laying out a wide, cool swath of illumination so that I could see the entire area.

The Modus 1's soft push-button power control takes some getting used to, but it has a nice feel. This is a fine tool to add to your toolbelt, for those situations when you need to shed a little (or a lot) of light on the subject. Purchase the Modus 1 (and heftier Modus 2) at www.myiconlight.com.



Perhaps a bribe is in order?



Wink, wink

User Moment of the Month

by Jason Yagelnesky

I work at a university Help desk in Saskatchewan, Canada. One day, I received an email message from a client that read, "Hi, I am unable to see any new messages in my Inbox. Can you help?" I began an email response, only to find that the user hadn't provided any contact information—and had emailed from the problem account.



HOB RD VPN Desktop-on-Demand

Don't Go To My PC – Go Directly To Your PC!

With HOB RD VPN Desktop-on-Demand you can access your desktop from anywhere. If your computer has been powered down, you can remotely start it.

SSL-encrypted and highly performant

The data are encrypted with SSL, and the default port 443 is used.

The RDP protocol is used for obtaining access with optimum performance.

Clientless and platform-independent No administrator rights required

This HOB software is browser-based and platform-independent, meaning you can access your data from Windows, Macs or even Linux machines.

The highly performant RDP Java client HOBLink JWT is integrated in HOB RD VPN.

Easy data transfer and local printer support

When you access your desktop, you can use the clipboard and print or transfer files over the Local Drive Mapping feature.

Desktop-on-Demand for Windows, Linux and Mac

The desktop acts as an RDP server for Windows XP, Windows Vista and Windows 7 (Exception: the Home Editions).

Even if your desktop is not running a Windows OS, HOB has a solution: HOB X11Gate for Linux or HOB MacGate for Mac OS X.

These add-on components from HOB allow you to access non-Windows desktops over the highly performant RDP protocol.



HOB RD VPN *Secure Remote Access*

The Secure and Comprehensive Remote Access Software Suite!

HOB RD VPN is a software product, not a hosted service. This means your data remains fully in your hands, under your control and nobody else's.

HOB RD VPN also provides:

Remote Desktop Services (RDS)

VDI (Virtual Desktop Infrastructure)

Web Server Gate for accessing internal Web servers

File exchange with Web File Access

VT / SSH as a Java client (ideal for administrators)

HOB PPP Tunnel for universal network access

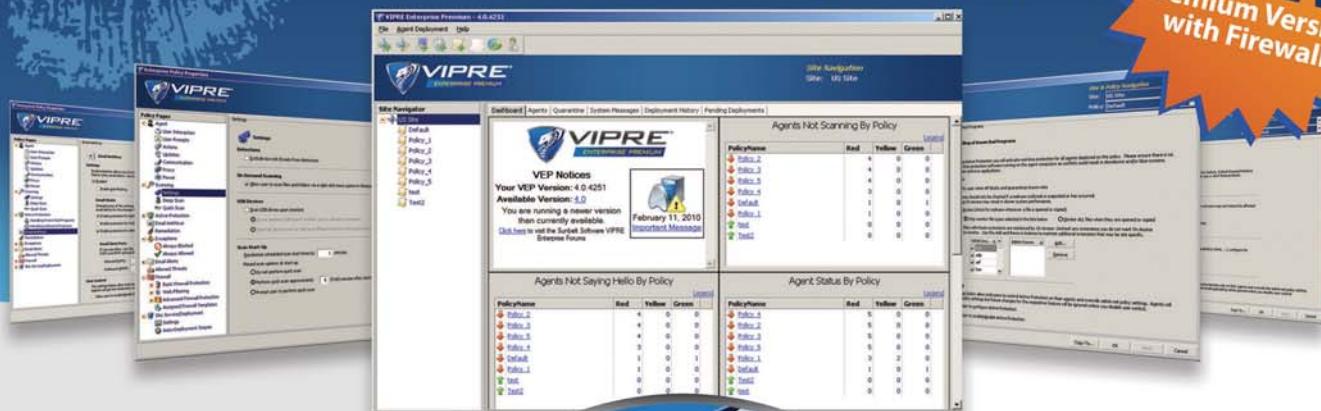
Standard emulations in Java (3270, 5250, VT, 9750)

www.hobsoft.com/DoD2

HOB RD VPN is Common Criteria certified*

Kiss your antivirus bloatware goodbye

NEW
Premium Version
with Firewall

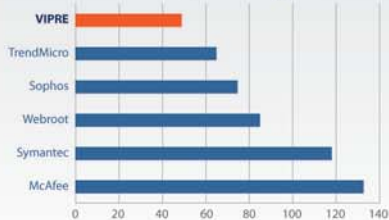


VIPRE

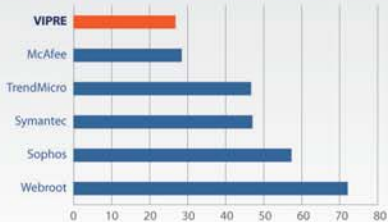
TEST DRIVE

ENTERPRISE PREMIUM

Memory Used During Scan



CPU % Used During Scan



How does your current software compare?

VIPRE Enterprise scans at a brisk 13.95 MB/sec and uses just 27% of CPU and 50 MB of RAM. In idle, it uses a mere 13.3 MB RAM with a disk footprint of just 113 MB. You'll hardly notice it's running!

Special Competitive Upgrade: 50% Discount!

Until now, antivirus engines have been Franksteins, bolted together from bits and pieces of different products. They're slow, full of bugs, and hard to manage.

VIPRE Enterprise Premium is a revolutionary new approach. It combines high-performance antivirus, antispyware, and desktop firewall into a single agent so you get comprehensive endpoint malware protection with low system resource usage. It's fast, powerful and easy.

Plus, advanced anti-malware technology protects your system against the new wave of malware threats. No more juggling multiple programs. No more dealing with user complaints about slow workstation performance.

- **COMPLETE!** All-in-one protection from today's malware.
- **FAST!** High-performance and low impact on system resources.
- **EASY!** Manage everything easily from one command screen.
- **RELIABLE!** Configurable, real-time monitoring technology.
- **AFFORDABLE!** Ask for a quote with our 50% competitive upgrade discount!

Why struggle with slow resource hogs when you can manage ALL your malware threats with one fast, easy application?

Curious? Download your FREE copy of VIPRE Enterprise Premium and give it a test drive.

When you compare VIPRE Enterprise Premium to Symantec, McAfee, Trend Micro or whatever antivirus program you're using, **you WILL want to switch!** Don't worry, though. You can get VIPRE Enterprise Premium with a **50% competitive upgrade discount!**



Sunbelt Software

Plus we will buy out your existing maintenance contract for 1 year!

Download now: **www.TestDriveVipre.com**

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.SunbeltSoftware.com sales@sunbeltsoftware.com

© 2010 Sunbelt Software. All rights reserved. VIPRE Enterprise is a trademark of Sunbelt Software. All trademarks used are owned by their respective owners.

Discount available on new licenses only for a limited time. Buy-out offer good on contracts up to 1 year. Subject to change without notice. Contact your Sales Representative for details.